A Cybersecurity Strategy Anyone Can Understand

As a cybersecurity professional, I often talk about the importance of good planning. A good cybersecurity strategy can help stand directly between cybercrime and your business.

Whether you are tasked with creating a cybersecurity strategy for your business or you just want to know how to follow a good cybersecurity strategy, it's important to understand the basic elements of an effective cybersecurity plan.

The National Institute of Standards and Technology (NIST) lays out the framework of cybersecurity by breaking it into five components: identify, protect, detect, respond and recover. Each part represents a crucial role in cybersecurity success.

Identify

The identification phase is where you look to get a greater understanding of the cyber risks to assets, systems, data, capabilities and people. This is where you identify what needs to be protected, what's most vulnerable and what you need to protect yourself from.

When starting out, deciding what to protect can seem overwhelming, but you can make it easier on yourself by understanding how your organization generates revenue. This should give you a good idea of what is crucial.

From there, map out the functions and systems that, if breached, could interfere with revenue generation. Of course, you also want to understand what you are legally required to protect.

You also want to take note of any sensitive information your organization contains and who has access to it, as well as how it is stored and managed. The severity of a cyber breach and associated fines depends largely on what type of sensitive information was compromised.

Protect

After identifying what is crucial to your business, you need to outline safeguards to maintain the business operations of those critical functions. This could include anything from cybersecurity awareness training for employees to VPN remote work solutions that allow employees to work securely from home. Detail any protective measures your business needs to take while focusing on the critical parts of your business that were discovered through the identification phase, and then put a plan in place to make it happen.

Detect

Even with properly identified protection measures in place, it is crucial that you have the ability to detect a breach in the event something slips through your defenses.

One of the things that I consistently hear from my contacts in the cyberthreat intelligence community is that the faster you can detect and respond to a cyber breach, the better chance of business survival.

A couple of good questions to ask yourself in this stage include:

• What is our company's capability to detect a breach?

• How do we know our organization is not being breached right now?

Respond

You should also have a detailed and practiced cyber breach response plan. This way, once you detect a breach, you can act on it immediately. Make sure to include exactly when and how the company will contact the media, employees, partners and customers.

Considerations for this stage include asking yourself the following:

• Which breaches require notification?

• Who needs to be notified of the breach?

• When does notification need to happen?

• How does the notification need to be delivered?

Having a solid understanding of your legal requirements regarding breach notification will go a long way in protecting your business from pricey fines.

Ideally, when responding to a cyber incident, your first call should be to a breach coach who, among other things, will be able to help you navigate the legalities of what is required for your breach response. This is a relationship that is often put in place through your cyber insurance contract.

However, simply having a response plan is not enough; it also requires practice with your entire team. Rehearsing your plan will allow you to not only get better at it but to also spot weaknesses in the plan.

Lastly, always make sure you have a paper backup of your response plan. The last thing you want is to put all that work into a carefully thought-out response strategy only to be blocked from it because of the breach you've just been hit with.

Recover

No cybersecurity strategy is complete without a plan for recovery. Here are some key questions to ask yourself for this part of the plan:

• **Do we have cyber insurance?** Although cyber insurance isn't a cybersecurity solution, it's the only pathway to financial recovery after a breach, and as such, it fits in perfectly in the recovery stage of the NIST Cybersecurity Framework.

• **If we have cyber insurance, do we know what it covers, and, more importantly, do we know what it doesn't cover?** Like any insurance plan, you need to find one that's right for you.

• **Do we have access to a cyber breach coach?** As mentioned above, in the event of a breach, a breach coach should be the first call you make. They can also aid in your recovery.

Last of all, remember that when it comes to implementing and following the NIST Cybersecurity Framework, it's just like the old saying goes: A failure to plan is a plan to fail.