5 WAYS TO REFRESH YOUR POST-PANDEMIC CYBERSECURITY POSTURE

cipher
a PROSEGUR company

DOCUMENT ACCESS LEVEL

OUTLINE

5 WAYS TO REFRESH YOUR CYBERSECURITY

A Changing World

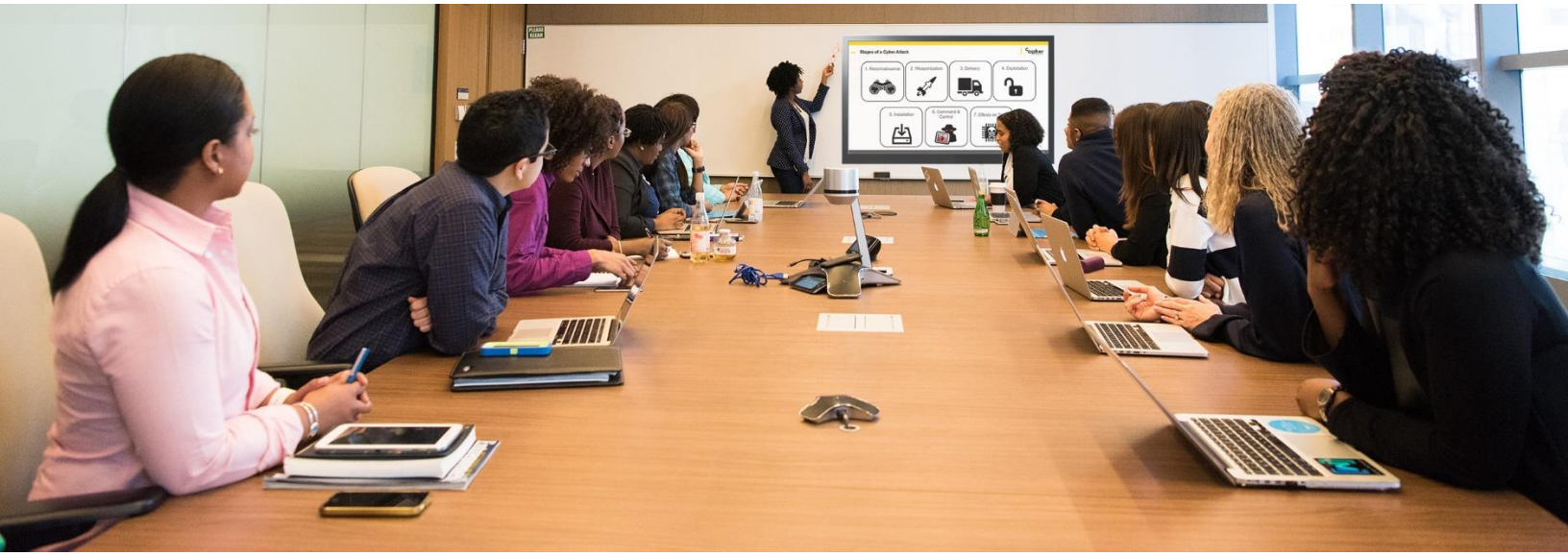
As the pandemic thankfully wanes in many parts of the world, people are looking ahead and hoping to shake off the malaise of COVID-19. Complacency can set in if systems and habits do not change. New habits, attitudes, and outlooks can help people stay energetic and focused.

The world of cybersecurity is constantly changing. Attackers are adapting their technology and tactics to infect victims and make money. Every day, new techniques and exploits are being developed.

During the pandemic, many initiatives were sidelined due to the complexities of remote work. The pandemic also has given rise to a new kind of cybersecurity, targeting remote workers Now that employees are back in the same physical room, details can be hashed out without a video call.

The elements of a company's IT and cybersecurity posture should undergo routine reviews, audits, and enhancements. This white paper will cover areas that a company should look into, in order to update and refresh their cybersecurity posture. Cipher Chief Technology Officer for North America David Rickard brings his expert analysis into the topic as well.

1. Perform Security Awareness Training



Solidifying a culture of cybersecurity begins with education and awareness. Most people want to comply with security policies, they just need to know what they are and the rationale that supports them. User awareness is a key ingredient, one that many would say is the cornerstone of any security program.

Holding the training in-person will help get the message across. The undivided attention gained from being in the same room can get the important messages across. The training should be targeted to the audience. For the everyday employee, topics in the awareness training will be more basic.

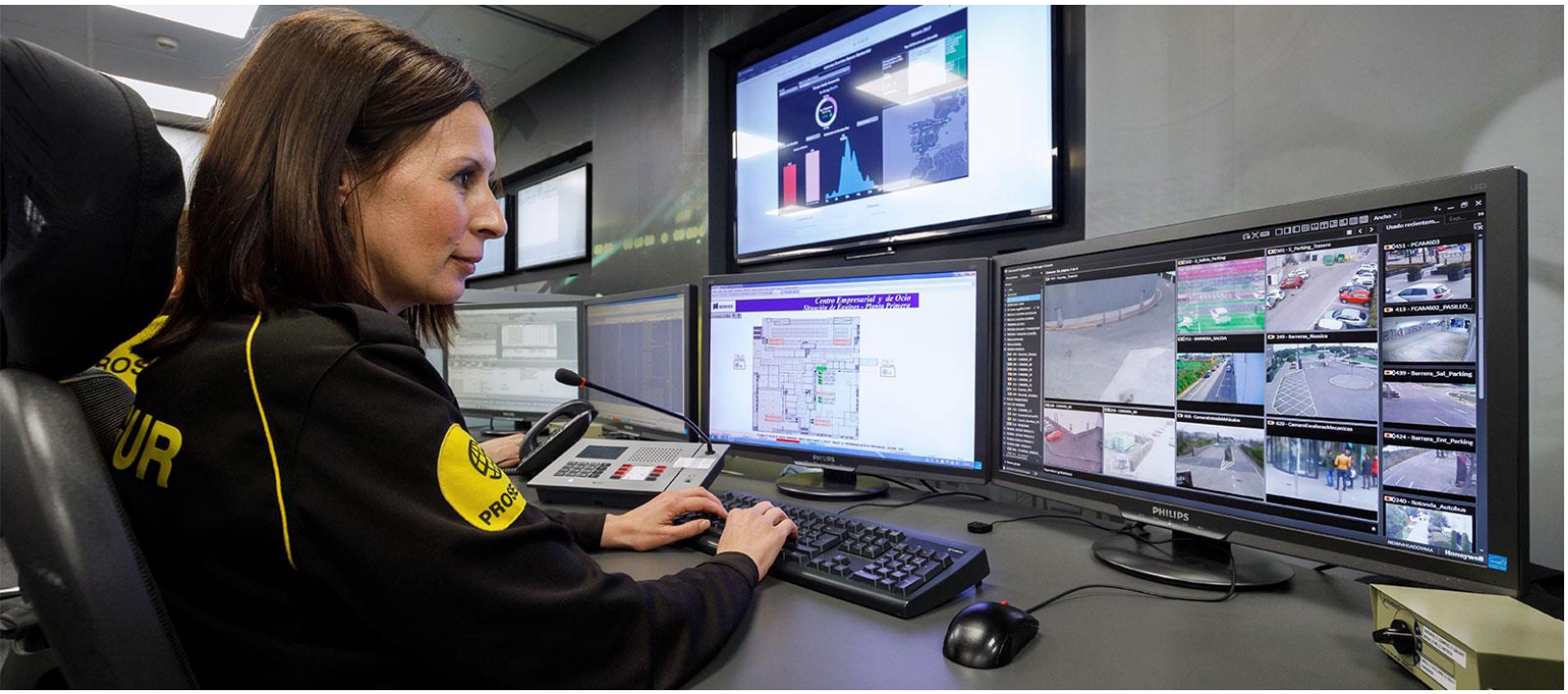
Conversely, the pandemic has shown some benefits of remote training. “Remote training works and provides a record of who attended,” said Rickard.

Core Concepts in Cybersecurity Awareness Training

- Email safety and phishing
- Social engineering
- What information to disclose externally, with special attention paid to Personally Identifiable Information (PII)
- Password best practices and Multifactor Authentication (MFA)
- Acceptable use of business computers and devices
- Appropriate use of Social Media

The level of detail in the training and will be more if the role is more technical or involves sensitive information.

Physical Workplace Security Training



As people shift to being in-person, brushing up on the basics of physical security in the workplace is a good idea. The physical and digital worlds are interconnected. If a threat actor can gain physical access to an unlocked computer, they can wreak havoc.

Make sure your physical access controls are solid. Ensure access cards or keys are in the right hands. Establish clear policies when it comes to visitors. Do not allow tailgating into offices. Document and enforce a clean desk policy. Consider using remote video monitoring to make sure training is followed if your workplace details merit it.

2. Review User Access

Keeping user records updated is important since every login represents a vector that threat actors can use to hack into a system. A survey of IT professionals found that 82% said their business has been exposed to a risk due to poor identity and access management. Refresh your user access records and protocols when people return to the office.

If an employee left during the pandemic, their accounts should be inactivated and/or removed. Ghost Account is the term for accounts that are in a company's directory that are not being used by a person. These accounts have credentials and access, but no purpose to exist.

Pay attention to the level of access employees have. Use the principle of "least privilege" to manage accounts. No users should have administrative access unless absolutely necessary. The user's privileges should be based on what access they need to specific files. "Access should be audited and reviewed on a quarterly basis. If a user doesn't access something to which they have permissions for a 6 month time period, for instance, that permission should be removed," said Rickard.

The AAA Framework is an easily understood framework to use as access policies are set. The components are:

Authenticate

Authenticating users is the first step in a secure identification system. The system needs to make sure the person accessing a system is who they say they are. The method of authenticating a person can fall into what they know (passwords), what they have (mobile device), or who they are (facial or other biometric identification).

Authorize

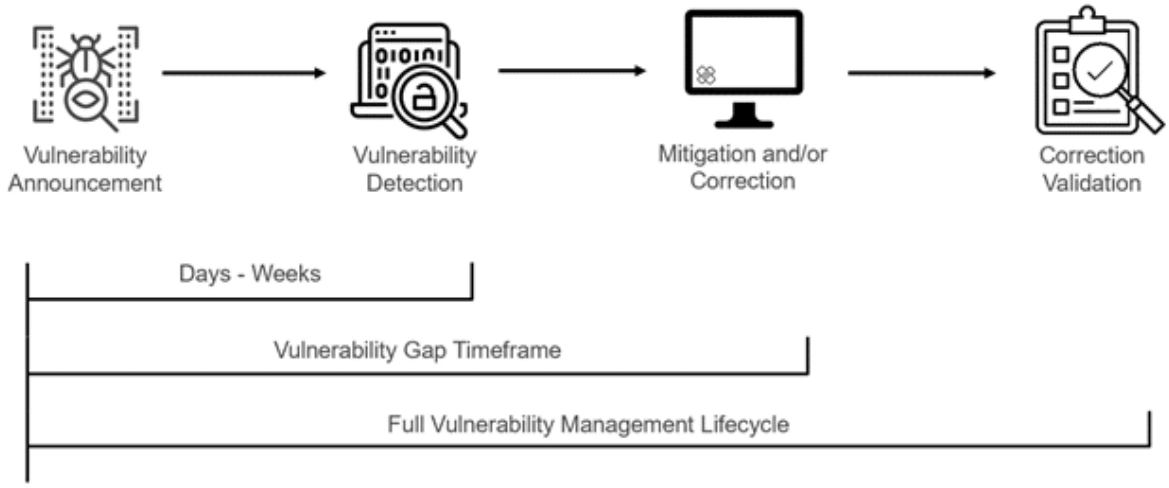
Determining the type of authorization employees have within a network is the next step. "The right people should have the right access level to different assets and data stores, based on a need-to-know, and reviewed regularly," said Rickard.

Account

After a person begins logging into a network and working, their usage should be monitored. AAA logs can be directly consulted for forensics reporting, as long as they've been retained, the logs of employee actions can also be monitored by working with a company that utilizes. Security Information and Event Management (SIEM) software or using a SIEM on your own.

3. Patch Your Software

“A vulnerability management program is a must-have, along with having an inventory of hardware and software assets. Knowing what vulnerabilities exist enable pursuit of timely patching for those vulnerabilities. The length of time it takes between realization of a vulnerability and remediation of it through applying vendor patches amplifies risk per the length of time it takes to achieve,” said Rickard.



The Ponemon Institute calculates that 60% of breaches were linked to a vulnerability where a patch was available, but not applied. A solid patch management system starts with a comprehensive discovery and inventory of your systems using tools to automate the process. You could devise your own patch management strategy and plan for managing patches and upgrades. The consulting services of an service provider can also help you handle these changes.

A comprehensive security strategy will include automated software patches and eliminates the potential for cybercriminals to exploit your software and OS vulnerabilities.

10 Steps to Patch Management

1. Create an inventory of all IT assets
2. Categorize by risk and priority
3. Utilize a test lab environment
4. Evaluate patch stability
5. Monitor and evaluate lab patch updates
6. Create backups on production environments
7. Implement configuration management
8. Roll out your patches to production
9. Ensure your patches are maintained regularly
10. Document Your Patch Management Process

CipherBox is an MDR (Managed Detection & Response) solution that helps with identifying vulnerabilities using Predictive Vulnerability Management.

4. Conduct a Table-Top Exercise

A table-top exercise is an event that tests the elements of an organization's cybersecurity and incident response process. To test the company, a scenario is first generated. Then the people responsible for cybersecurity perform the actions they would do if the threat was real.

A person or small group orchestrates the exercise. They look at what learning points to test and reinforce the topics after. The exercise could be a simple 15-minute exercise that is more discussion-based or a days-long event using actual company resources.

The Center for Internet Security has a list of six exercises that companies can perform. The exercises cover topics like malware, unexpected attacks, cloud security, and ransomware. Use these exercises to build your Incident Response Playbook.

Table Top Exercise Elements

- Discussion questions
- Processes tested
- Threat actor simulated
- Assets affected
- Areas of cybersecurity
- Different roles and responsibilities
- Lessons learned

"Practicing the playbook will improve your overall timeliness when an actual cybersecurity event occurs," said Rickard.

5. Work with a New Service Provider

Your company might already have a set list of cybersecurity vendors who you rely on to keep your company safe. Or maybe you are establishing a cybersecurity program from the ground-up.

The competition for cybersecurity professionals is also very intense, and companies might need to utilize outside resources to maintain their secure posture. Limited staff means less analysts monitoring and responding to alerts. There might be no analysts hunting and investigating, which results in a greater chance of a successful breach.

A new service provider can be used to give your organization a fresh look. It is a best practice to use different providers for services like penetration tests for example. Different service providers have unique methods to accomplish their work. Old habits are hard to break. These habits could make your company a target for a breach.

Choosing a solution provider is a large commitment. Evaluate your options using a common criteria.

Areas to Consider When Choosing a Cybersecurity Solution Provider

- ☑ Pay attention to how long the provider has been in business.
- ☑ Talk with current customers to get testimonials.
- ☑ Understand what technology they will bring to bear.
- ☑ Consider the service you will get from the company with regards to the availability of phone support, regular meetings, and reporting.
- ☑ Compare the price of the service, but at the same, understand that cost of a breach or cyber incident can vastly outweigh the incremental differences between vendors.
- ☑ Having one vendor for multiple needs could also be helpful, so look at their whole portfolio.