The 3 Stages to Improve Your Cybersecurity Strategy: People, Processes & Technology

CES' Cybersecurity Product Suite provides staff with the resources and knowledge to defend a company's front line, while helping to strengthen processes and protect connections through scalable layers of security.

Challenge

Picture this: it's Monday morning; you just returned from a weeklong break and began skimming a massive backlog of emails. While hastily catching up, you click on a questionable link indicating an expired password, realize your mistake, delete the message, and casually continue scrolling, never mentioning the situation to IT or a supervisor. While alarming, this honest oversight can happen to almost anyone, which is perhaps the point. Because now, imagine how often scenarios like this happen throughout your entire team week after week.

The unfortunate truth is it takes just one click, and an attacker can access your entire infrastructure. What's worse? Breaches are not always blatant, and it can take up to a week for you to even realize you have been infiltrated. With cybercrime on the rise unlike ever before, right now is when businesses should be scrambling to scale their security posture. Especially since...

There is an estimated ransomware attack every 11 seconds

More than 3 billion malicious emails are sent every day

1-in-4 employees confessed they have clicked on a phishing email at work due to distraction

The Solution

When it comes to cybersecurity, businesses must start thinking critically and holistically, focusing on the three main pillars that help ensure a comprehensive cybersecurity strategy...

1. People

While many teams work 100% from home and others prefer hybrid models, most are unaware of the added cybersecurity risks while working remotely. For instance, did you know...

- 56% of employees use personal, potentially unprotected devices when working offsite, and 70% of office workers admit to using work devices for personal tasks
- 20% of organizations faced a security breach because of a remote worker
- 25% do not know the security protocols on their devices
- 20% said their IT department provided zero tips for working remotely
- Remote work caused the average cost of breach to increase by $137,000

Employees are your first line of defense wherever they work, making Security Awareness Training (SAT) one of the most important investments you can make for the future security of your organization. Use Security Awareness Training to quickly educate staff on...

- The risks and vulnerabilities facing their business environment
- The tools they can use to minimize these risks and vulnerabilities
- The mechanisms a company puts in place to ensure their knowledge is kept current

What is Security Awareness Training and How Does it Work?

Designed by admins for admins, our convenient training platform manages social engineering problems with an easy-to-use console that utilizes...

1. The world's most extensive training library: Train employees using the world's largest library of security awareness training content available
2. Baseline testing: Access baseline testing to assess the phish-prone percentage of users through a free simulated phishing attack
3. Simulated Attacks: Utilize fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates
4. Detailed results: Gain enterprise-strength reporting with stats and graphs for both training and phishing

Security Awareness Training Benefits

- World-class customer assurance experience
- Advanced reporting and performance metrics
- Training specialized in all industry segments
- Access to engineers with certifications in security (CISA, CISM, CISSP, GCIH, CHFI, GCFA, ITIL, ISO27001 and more.)
- Additional layers of security: human awareness and vigilance

- Decreased number of cybersecurity incidents caused by human error and data misuse
- Recommendations for mitigating risks and risk remediation plans
- Management, logging, and reporting systems that meet the reporting and com pliance requirements

2. Processes

Once staff knows how to identify potential hazards, it's time to fortify your infrastructure. Strengthen your network by focusing on the processes that can help deter future threats—especially since 80% of data breaches can easily be prevented by practicing cyber hygiene. Use CES' Vulnerability Assessments to inform IT teams of potentially exploitable vulnerabilities on their computer information systems how to remediate them before any attacks.

What is Vulnerability Assessment and How Does it Work?

Teams can easily request and schedule scans using the secure CES portal. Designed to be a seamless and convenient process, our Vulnerability Assessments are deployed from a cloud management console that uses an internal scanning probe on your business network. Once the assessment is finished, employees can view technical and executive reports within the secure portal.

1. Cloud-based management console and local scanners are configured
2. For local scanners, organizations will provide the physical or virtual server(s) to install the scanner. CES will configure remotely
3. Automated requests for scanning exercises and customized reports through the portal
4. Detailed analysis of vulnerability scanning exercise with recommendations de livered through executive and technical reports published on the portal

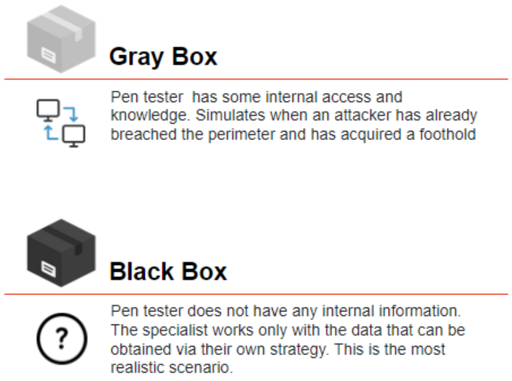
Vulnerability Assessment Benefits

- The industry's lowest false positive rate with six-sigma accuracy (0.32 defects per 1 million scans)
- More than 57,000 common vulnerabilities and exposures in its dictionary
- Assessments for threat intelligence and vulnerability prioritization
- Dynamically compiled plug-ins increase scan performance and efficiency
- Little configuration is needed; more than 450 pre-configured templates help you quickly understand where you have vulnerabilities
- Simplicity of deployment (easily scripted APIs for rapid provisioning of user accounts and access controls)
- Easy to use dashboards that provide deep insight into the effectiveness of pro cesses, plus customizable reporting capabilities that can be optimized to meet specific needs

Regularly exposing vulnerabilities has become essential, specifically since cybercrime can cost companies $1.79 million per minute. Precisely why Penetration Tests work to exploit any vulnerabilities found and determine the severity of each to gain access to the network. These comprehensive tests demonstrate how dangerous a flaw could be in an actual attack rather than finding every fault in a system.

What is Penetration Testing and How Does it Work?

Penetration Testing and Vulnerability Assessment are often combined to achieve a complete analysis and provide a detailed picture of the flaws in computer information system and the associated risks. With Penetration Testing, users have access to two levels of analysis...



Gray Box

Pen tester has some internal access and knowledge. Simulates when an attacker has already breached the perimeter and has acquired a foothold

Black Box

Pen tester does not have any internal information. The specialist works only with the data that can be obtained via their own strategy. This is the most realistic scenario.

Penetration Testing Benefits

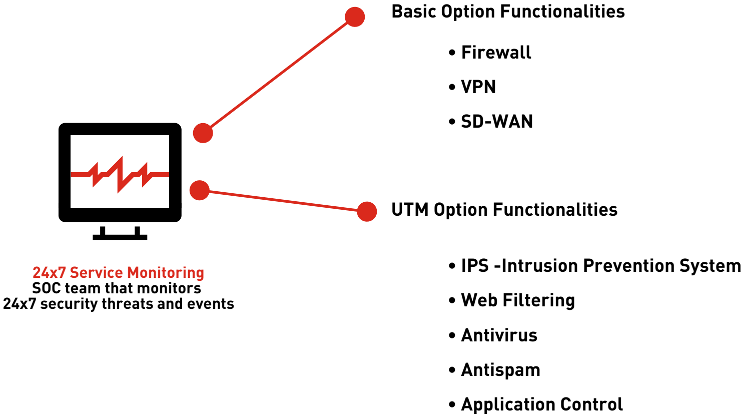
- Discover personalized recommendations and methods for patching security gaps to prevent future incidents
- Establish a safe perimeter of the customer’s network at all points of contact with the public internet
- Create a security strategy focused on risks and aligned with business objectives
- Deliver accurate information on the status of the local corporate network for decision-making
- Reduce economic losses and lessen damage to your reputation after a cyberattack
- Eliminate false positives and know which vulnerabilities are genuinely exploitable
- Validate compliance with security policies regarding people, processes, and technology within your organization
- Access specialized support from over 600 cybersecurity analysts with experience in global security threats
- Gain industry-specific methodologies based on international information security standards
- Utilize over 1,200 certifications, including CISA, CISM, CISSP, CCNA, ITIL, ISO27001, GCFA, CHFI, and more

3. Technology

Once your team has the resources and training to succeed, and their processes are refortified, it's time to strengthen and protect your network. Managed Secure Business Internet (MSBI) allows business customers to transfer risk to a state-of-the-art security operations team while at the same time reducing costs by outsourcing essential security functions. Help eliminate cyber threats, improve customer service, and increase productivity with customizable layers of security that integrate 24/7 monitoring, a next-generation firewall, scalable Unified Threat Management (UTM), and more.

What is Managed Secure Business Internet and How Does it Work?

In addition to minimizing cyber threats, MSBI's customization enables multi-location network scalability with added layers of security to provide businesses with faster, more secure networks.



Basic Option Functionalities

- **Firewall**
- **VPN**
- **SD-WAN**

UTM Option Functionalities

- **IPS -Intrusion Prevention System**
- **Web Filtering**
- **Antivirus**
- **Antispam**
- **Application Control**

24x7 Service Monitoring
SOC team that monitors
24x7 security threats and events

Managed Secure Business Internet Benefits

- Managed 24/7 network traffic monitoring through our Security Operations Center (SOC)
- Next-generation firewall
- LTE failover
- VPN
- SD-WAN
- Scalable UTM features
  - Antivirus
  - Antispam
  - Intrusion prevention
  - Application control
  - And more

Already have a business internet connection?

Add all the scalable layers of security from MSBI without switching providers with a Managed Perimeter Security solution. Managed Perimeter Security provides the resources to raise your security posture and manage your business network. Help reduce cyber threats, enhance customer experiences, and ensure your company's reporting data is accurate and compliant with government, industry requirements, and regulations.

The Takeaway

With billions of phishing emails sent daily, having a holistic cybersecurity approach has become essential to operating online. By (1) training employees on the potential risks, (2) assessing network vulnerabilities (3) testing your network and those vulnerabilities, (4) and protecting your connection with layers of security, you help ensure your team has the knowledge and resources to defend your network 24/7.

Cybersecurity
info@usclaro.com
833-992-5276

Claro
Enterprise Solutions