According to a recent Gartner report, “The Urgency to Treat Cybersecurity as a Business Decision,” “CTOs need to consider the risks, security priorities and investments that impact their business outcomes.” A key recommendation in the report is that CTOs need to focus on IT cost optimization, finance, risk and value to optimize risk and business performance and to improve cybersecurity readiness by treating it as a choice and a business decision. One way to develop an outcome driven cybersecurity strategy is to employ The CARE Standard for Cybersecurity outlined below.

**THE CARE STANDARD FOR CYBERSECURITY**

Cybersecurity strategy must be an ongoing, dominant priority for all businesses as we adapt to a post COVID-19 world, where the lines between work and home are increasingly blurred. The importance of cybersecurity continues to accelerate as internet access expands as employees work from home using personal hardware and consumer security products. Risks increase as multiple devices beyond PCs and phones to include tablets, wearables and smart network devices, are added to the mix. Meanwhile, hackers and malicious actors are increasing their sophistication.

Consider the existential threats that a hack could have to your business. Beyond damaging your professional reputation, including diminished trust from your clients, you could be faced with lawsuits, stolen monies and other financial burdens that could impact the viability of your business.

**C** **CONSISTENT:** Do your controls work the same way over time?

**A** **ADEQUATE:** Do you have satisfactory and acceptable controls in line with business need?

**R** **REASONABLE:** Do you have appropriate, fair and moderate controls?

**E** **EFFECTIVE:** Are your controls successful in producing the desired or intended results?

Ultimately, these are value judgments that must be credible and defensible. In these four characteristics are a myriad of opportunities to do what is best for the organization. It supports the creation of a balance between protection and running the business. It also embodies the incentive to build a better security capability that delivers better outcomes, not just spend more money on security.
While the threats may seem daunting and never-ending, a holistic strategy for your organization can be implemented with relative ease and provide assurance to you, your employees, and your clients. Your cybersecurity strategy should include looking at seven separate layers.

1. **INTERNET FILTERING**

   The vast majority of threats originate from the internet. You should evaluate your policies in three key areas:

   **A. Email Filtering**
   
   How does your organization filter malicious email? Relying on junk mail filters alone may not be enough. You should consider additional mailbox protection from your email provider or a third-party vendor. These tools will significantly decrease fraudulent emails.

   **B. Web Filtering**
   
   Are you users inadvertently landing on malicious sites? Are they using business resources to access social media for personal use, perhaps exposing company information in the process? Consider adding a DNS filtering tool; these products dynamically block known malicious sites and also allow you to configure policies to restrict user access to non-business sites.

   **C. Hardware Firewall**
   
   Any corporate network must be behind a physical firewall device. This will limit inbound attacks to your network. Robust firewalls will also contain monitoring and intrusion detection tools.

2. **ENDPOINT DEVICE PROTECTION**

   Your endpoint devices (PCs, phones, tablets, etc.) must be secured. You should consider implementation of the following tools:

   **A. Antivirus Filtering**
   
   Virus threats continue to evolve, and better antivirus tools include intrusion detection. Business antivirus solutions should include monitoring of your environment.

   **B. Antimalware Tools**
   
   Malware attacks now include ransomware – malware that cripples your network and devices until the malicious actor is paid a ransom. Antimalware solutions supplement antivirus filtering by providing an additional layer of security.

3. **ACCESS CONTROL**

   User access needs to be appropriately considered and limited.

   **A. Passwords**
   
   Do you have strong password requirements? Are you providing your users with a secure method of storing their passwords? You may wish to consider biometric authentication or hardware authentication.

   **B. Multi-Factor Authentication (MFA)**
   
   We consider MFA to be the best tool to significantly increase your organization’s security with minimal effort. Read more in our MFA Think Piece.

4. **DATA PROTECTION**

   How do you protect the data on your PCs and network, and the data that you transmit?

   **A. Data at-rest**
   
   Do you have security controls to sensitive files on your network? This may be as simple as limiting access from all users or enabling file-level passwords. All data should be encrypted.

   **B. Data in-transit**
   
   Do members of your organization send sensitive information? Consider implementing an encrypted email solution. Cloud-based file storage should have data loss prevention policies enabled.
5. PATCHING POLICIES
Old software can be a hacker’s goldmine as vulnerabilities can be exploited to gain control of your PCs and network.

A. Software updates
Does your organization have a formal patch management solution? These solutions can aid in the deployment of operating system, browser, and application updates.

B. Legacy systems
Is it time to retire the document management system your organization setup in 2005? What other home-grown or custom software exists on your network from many years ago? Software tools must be continually evaluated to ensure that they are receiving security updates. Outdated and unsupported systems should be retired.

6. BUSINESS CONTINUITY
The pandemic has revealed just how critical it is to maintain business operations despite external challenges. Disaster recovery plans have never been more vital, and must consider backups and testing.

A. Backups
How is your data backed-up? Do you have local backups, cloud-based backups, or both? How current are your backups and how far back do you maintain history? Can your backups survive a ransomware attack?

B. Testing
Do you test your backups? How about your business continuity plans? Testing can expose items that need to be improved and provide you and your employees “muscle memory” so that recovery can proceed with minimal hiccups.

7. USER EDUCATION AND AWARENESS TRAINING
At the end of the day, the best security tools can amount to nothing if your users are inadvertently creating exposure for your organization because of a lack of cybersecurity awareness.

A. Initial orientation and ongoing training
Provide your new hires with cybersecurity training and require employees to do ongoing training at least annually. There are a variety of organizations that can provide supplementary training regimes.

B. Fiduciary responsibility
Have you provided individuals that are responsible for moving monies additional targeted training? Consider your Accounting and HR professionals. At a minimum, ensure that they are knowledgeable about current email threats. Read more in our Fraudulent Email Think Piece.

Conclusion
The right cybersecurity strategy involves a multi-layered approach that is constantly re-evaluated. You may not be able to implement all of our recommendations immediately. Consider areas where your exposure is the highest and start there, and then phase-in elements as you move forward adopting the CARE Standard for Cybersecurity. Partnering with a managed services provider is another option to develop a strategy to optimize and secure your information technology.

Nick Holcomb is the Chief Technology Officer for Payroll Network, a premier HCM provider that brings together key workforce functions in one robust, easy-to-use platform. Nick has more than 20 years background in cybersecurity and 15 years of payroll/HR industry experience.

Mark Whisenhunt is a Principal with Computer Showcase, an IT solutions provider offering strategic consulting, managed services, and cloud solutions. Mark has been helping organizations embrace new technologies to improve capability, efficiency, and data security for more than 25 years.