LAUNCH SECURITY

Cybersecurity Checklist

Framework

- ❑ Response plan in place if attacked/breached
- ❑ Restrict employees from visiting non-business websites
- ❑ Ethical hackers attempt to break-in and report back
- ❑ Technology and data use policy in place and up-to-date

Culture

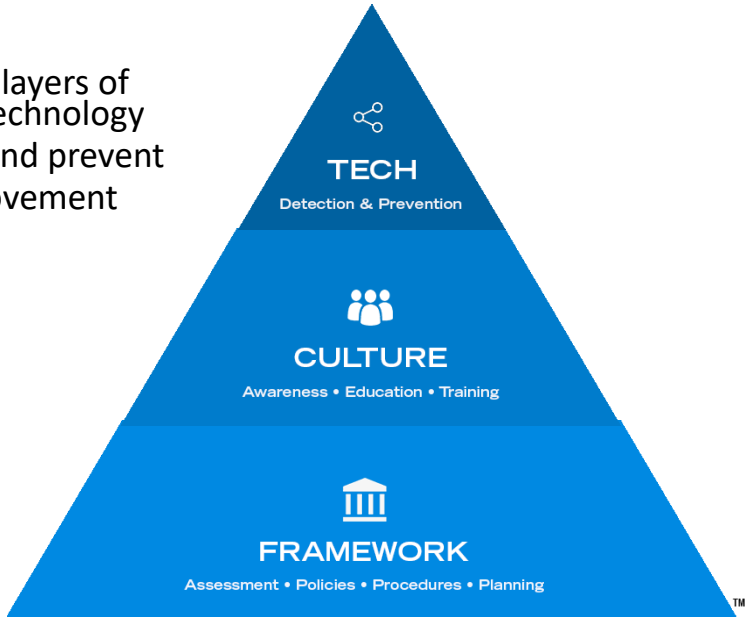
- ❑ Leadership meetings to discuss cybersecurity
- ❑ Train employees on threats and defenses
- ❑ Test employees with phishing simulations
- ❑ Promote cybersecurity awareness with posters and flyers

Technology

- ❑ State-of-the art protective software in place, not just antivirus
- ❑ Sensitive data at rest (e.g. on computers and mobile devices) *and* in-transit (e.g. email) is secured and encrypted
- ❑ Manage mobile devices globally (e.g. locate, freeze & wipe)
- ❑ 24/7 monitoring of activity with alerts and notifications

Program

- ❑ Includes three key security layers of Framework, Culture, *and* Technology
- ❑ Runs 24/7/365 to protect and prevent
- ❑ Model of continuous improvement



Cybersecurity Resources

The pool of information available on cybersecurity is deep. Visit **www.launch-security.com > Resources** where we provide a handful of key resources we hope you'll find useful, including:

Guides & Planners

- ✓ Cyber Security Planning Guide (FCC)
- ✓ Framework for Improving Critical Infrastructure Cybersecurity (NIST)
- ✓ Internet Security Essentials for Business 2.0 (U.S. Chamber of Commerce)

Online Portals

- ✓ National Cyber Security Alliance: StaySafeOnline.org
- ✓ Department of Homeland Security: Stop.Think.Connect.
- ✓ Federal Trade Commission: Privacy and Security

Tips & FAQ

- ✓ Cybersecurity Framework - Frequently Asked Questions (NIST)
- ✓ Ten Cybersecurity Tips for Small Businesses (FCC)
- ✓ 7 Essential Tips to Beat Phishing Scams (Norton)

Stay Connected!

Subscribe to the Launch Security blog to receive timely stories, quick tips, interesting facts, important statistics, and more.

*Sign up at **www.launch-security.com** or email **blog@launch-security.com***