Apptega

7 STEPS TO MAKE YOUR ORGANIZATION CYBERSECURITY ROCK STARS!

1

Read From the Same Sheet of Music

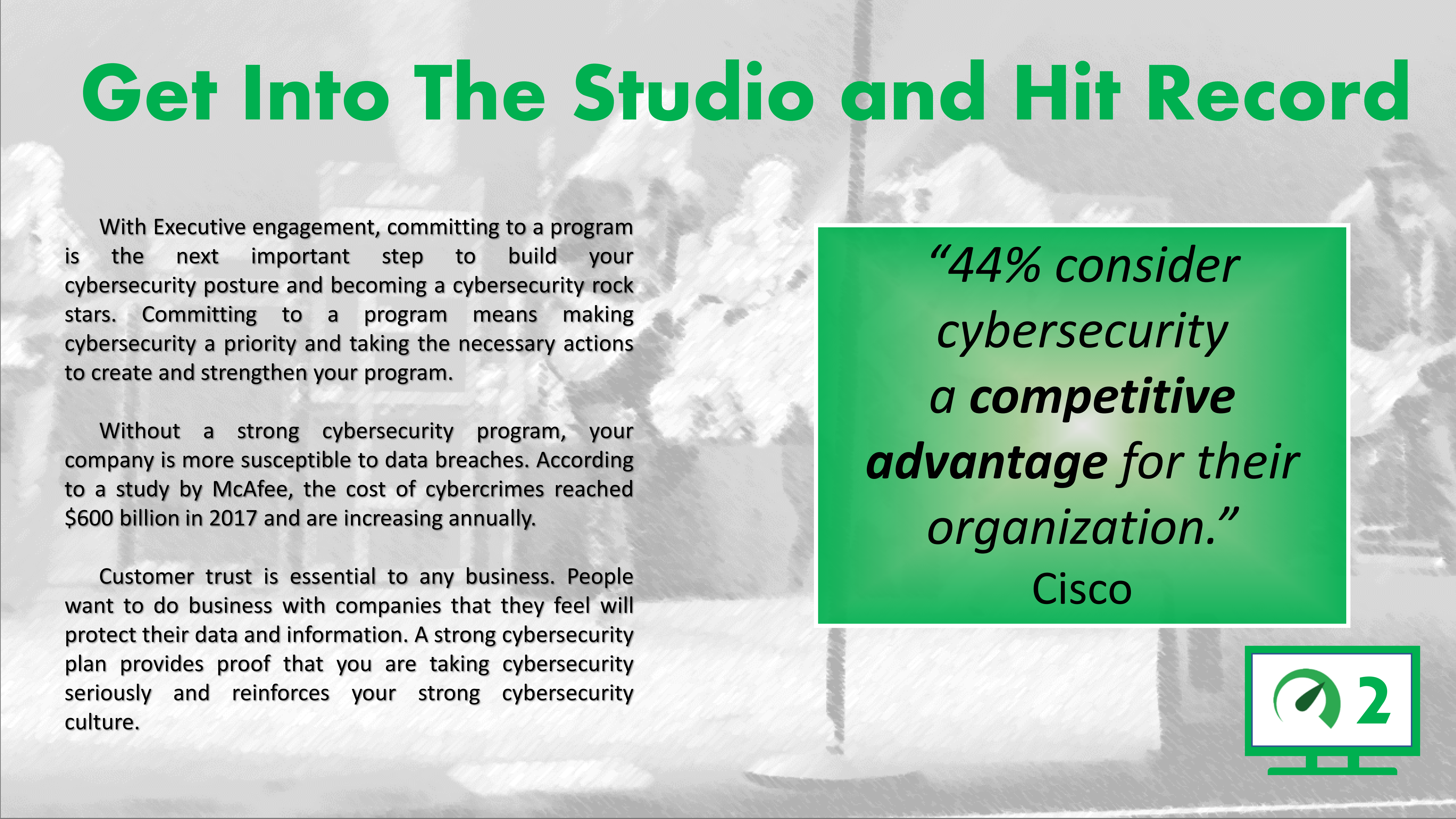
Even for non-regulated businesses, Boards and Executive Committees are asking about a company's cybersecurity posture. You must have an effective way to communicate progress towards an organization's plan. It is no longer just the responsibility of the IT team to ensure an organization maintains a strong cybersecurity posture.

Building a strong cybersecurity culture starts from the top. "The tone at the top sets an organization's guiding values," says Nicole Sandford, partner and national practice leader at Deloitte's Enterprise Compliance Services. "Properly fed and nurtured, it is the foundation upon which the culture of an enterprise is built."

By creating a written program with effective goals, you can start the process of holding people across the organization accountable to common goals and objectives. Without buy in from the top, it can be difficult to get organizational leader to prioritize projects needed to mature the cybersecurity posture.

> *"Creating and maintaining the right tone at the top is the bedrock…organizations can establish a tone at the top that truly binds the organization together."*
>
> Keith Darcy
> Deloitte

Apptega



Get Into The Studio and Hit Record

With Executive engagement, committing to a program is the next important step to build your cybersecurity posture and becoming a cybersecurity rock stars. Committing to a program means making cybersecurity a priority and taking the necessary actions to create and strengthen your program.

Without a strong cybersecurity program, your company is more susceptible to data breaches. According to a study by McAfee, the cost of cybercrimes reached $600 billion in 2017 and are increasing annually.

Customer trust is essential to any business. People want to do business with companies that they feel will protect their data and information. A strong cybersecurity plan provides proof that you are taking cybersecurity seriously and reinforces your strong cybersecurity culture.

> *“44% consider cybersecurity a* ***competitive advantage*** *for their organization.”*
>
> Cisco

2

3

> *"It's important to research the available security frameworks and balance the benefits and drawbacks of each approach."*
>
> IBM

Create Your Setlist

(choosing your framework)

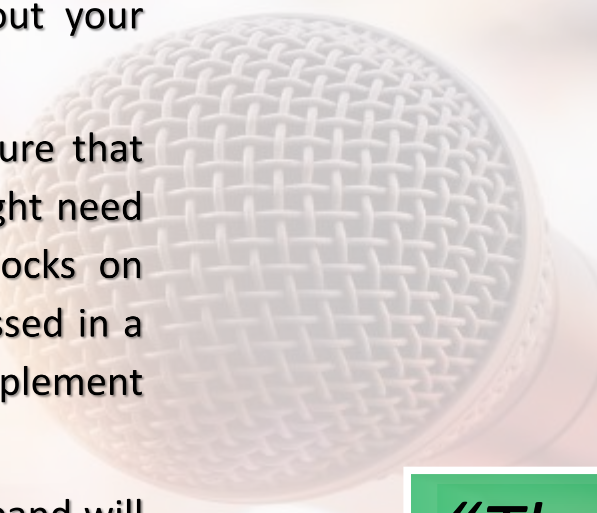
Different industries require compliance with certain framework(s). There are many frameworks out there like NIST 800.53, PCI, CIC Top 20, SOC2, ISO27001, HIPAA and GDPR to name a few.

- The Center for Internet Security (CIC) Critical Controls (formerly known as SANS Top 20) is often used as an initial framework as organizations start defining a cybersecurity program
- Many law firms are following ISO 27001 to show their clients a commitment to cybersecurity
- Healthcare organizations are required to maintain HIPAA compliance
- Businesses that accept, process, and store credit card information must meet requirements set by the Payment Card Industry Data Security Standard (PCI DSS).
- AICPA SOC2 is a compliance requirement for service organizations storing information in the cloud, such as SAAS providers
- Organizations working with and selling to the US government follow NIST
- Any business that collects or processes data from Europe directly or indirectly must be compliant with GDPR, with many of the articles relating to cybersecurity controls

Make sure your business takes the time to be familiar with the various frameworks and chooses one that meets the needs of your company, customers, and shareholders.

Improvise Your Jam

4



Every company is different and has unique security needs. To create the strongest possible program, you should start by choosing a framework to follow, but then add in what is unique about your business.

Businesses should set up controls, policies, and procedure that meet your specific needs. For example, some companies might need increased physical security measures. This could include locks on server rooms and security cameras that might not be addressed in a standard framework. Or, a company might want to implement additional restrictions on access to various internal systems.

Without defining and documenting these controls, your band will never be reading from the same sheet of music!

> *"There is no such thing as a one-size-fits-*
> *all approach to security."*
> IBM

Apptega

5

Everyone Plays Their Part

One of the largest gaps in a successful cybersecurity programs is a lack of accountability. Companies know they must take steps towards compliance, but without ownership many tasks are incomplete. Each sub-control is like a "mini-project" with tasks that need to be completed to improve compliance. It is essential that individuals across the organization know their specific responsibilities.

The ability to assign ownership creates individual accountability. Individuals can now be held responsible for completing specific tasks necessary to improve the company's cybersecurity posture. Social responsibility can be used to help reach company cybersecurity goals.

Tasks such as reviewing the company's policies should be reviewed on a reoccurring basis. If a company should review their policy once a year, setting a recurring task ensure the owner is reminded of their task and ensure it is completed.

> *"You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable."*
>
> Daryl White, DOI CIO

Apptega

6

Chart Your Progress

According to a Gartner study, "By 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity.” Companies of all sizes are more frequently asked to report on their cybersecurity program to executives, board members, and customers looking for validation that their information is being protected. There is confusion on what should and shouldn’t be included on these reports and how to obtain that information.

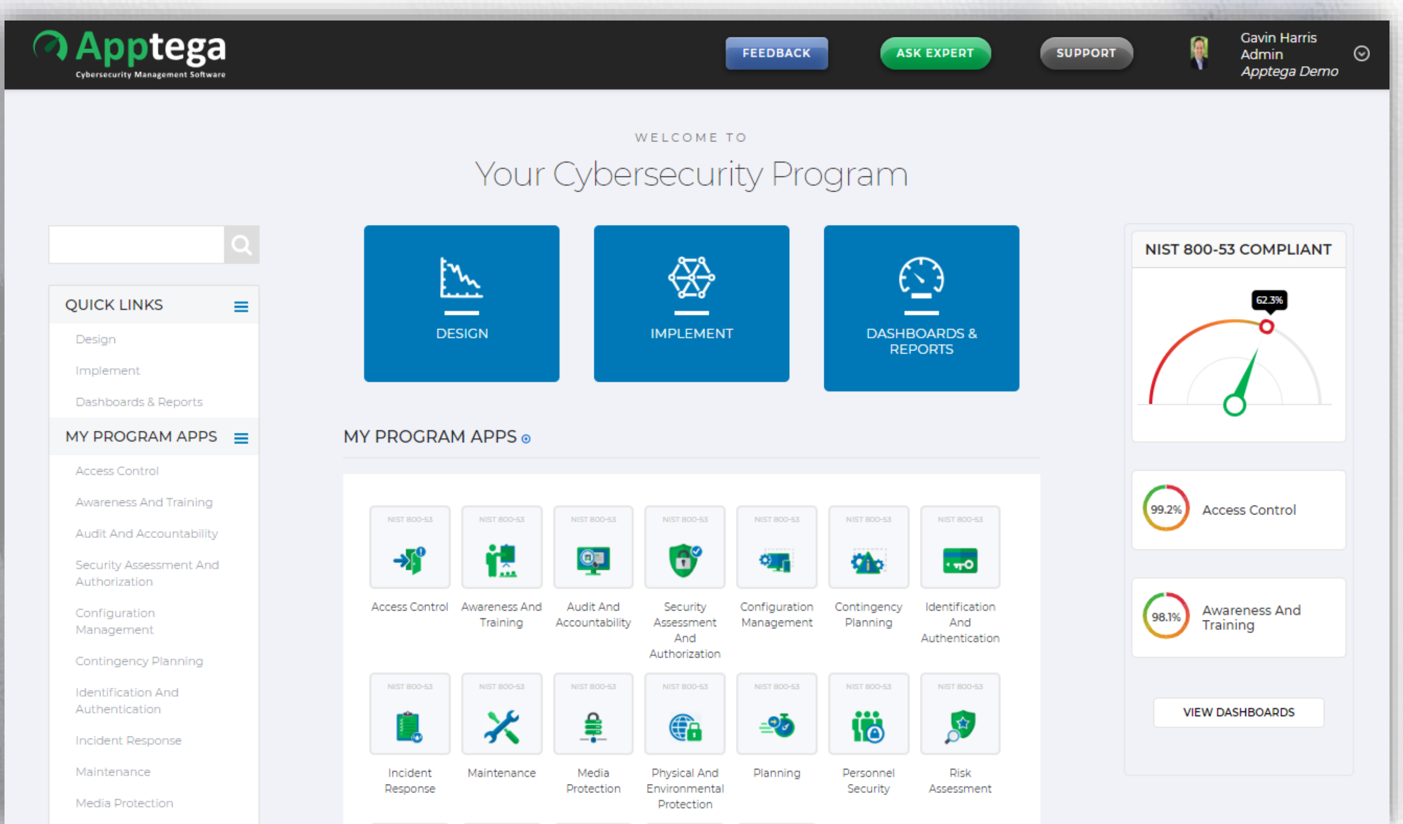
A major issue with reporting occurs with companies who are attempting to manage their cybersecurity program on Excel spreadsheets. With thousands of lines of information in these spreadsheets, it can be difficult, tedious, and require many hours to pull information on the company's cybersecurity posture. Excel spreadsheets are also a risk for data leakage and lost visibility when the creator of the document leaves the organization.

The reports generated should include the progress the company has made towards its compliance goals. The best reports do not simple list the steps taken, but quantify their progress and are simple and easy to understand. Boards and Executive Committees are not looking for details but high level review of program goals.

> *“It’s critical that security and risk management leaders supply board-relevant and business-aligned content”*
>
> Rob McMillan, Gartner

7

Get Back on the Road



The best way to think of cybersecurity is as an ongoing process, not a one-time project. By repeating these steps you can continue to strengthen your program and make it to the Hall of Fame.

Apptega provides a centralized, cloud based solution to build, manage, and report all aspects of your cybersecurity program. With Apptega, you can choose from industry specific frameworks or create your own. Create custom controls and sub-controls to meet your companies' unique needs.

Create accountability by assigning specific people ownership of the subcontrols. You can then create tasks within these controls and set up alerts for task that are reoccurring on a monthly, quarterly, or annual basis.

Reporting on your cybersecurity can be difficult and time consuming, with Apptega you can generate full program, board, and custom reports in seconds.

Apptega

Cybersecurity Management Software

www.apptega.com