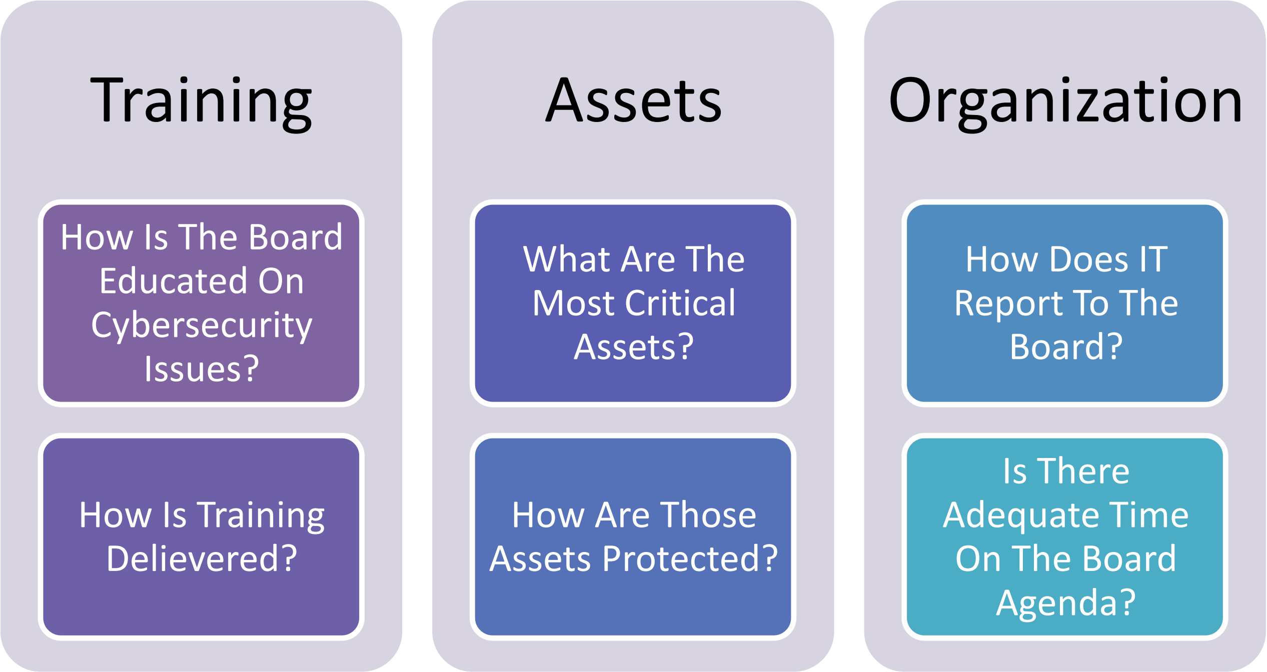
Integrating Cybersecurity into Day-to-Day Operations

Friday, November 15, 10:45 a.m. – Noon

Curt Creely, Partner, Foley & Lardner LLP
Aaron Tantleff, Partner, Foley & Lardner LLP
Peter Vogel, Of Counsel, Foley & Lardner LLP
Alicia Dietzen, General Counsel, KnowBe4
Miguel Clarke, Special Agent, Federal Bureau of Investigation
Chetan Bhatia, Vice President, Cyber Resilience, Stroz Friedberg, an Aon Company

Cybersecurity is an enterprise risk management issue: The Board should understand and approach cybersecurity as an enterprise risk management issue, not just an IT issue.



Training

How Is The Board Educated On Cybersecurity Issues?

How Is Training Delievered?

Assets

What Are The Most Critical Assets?

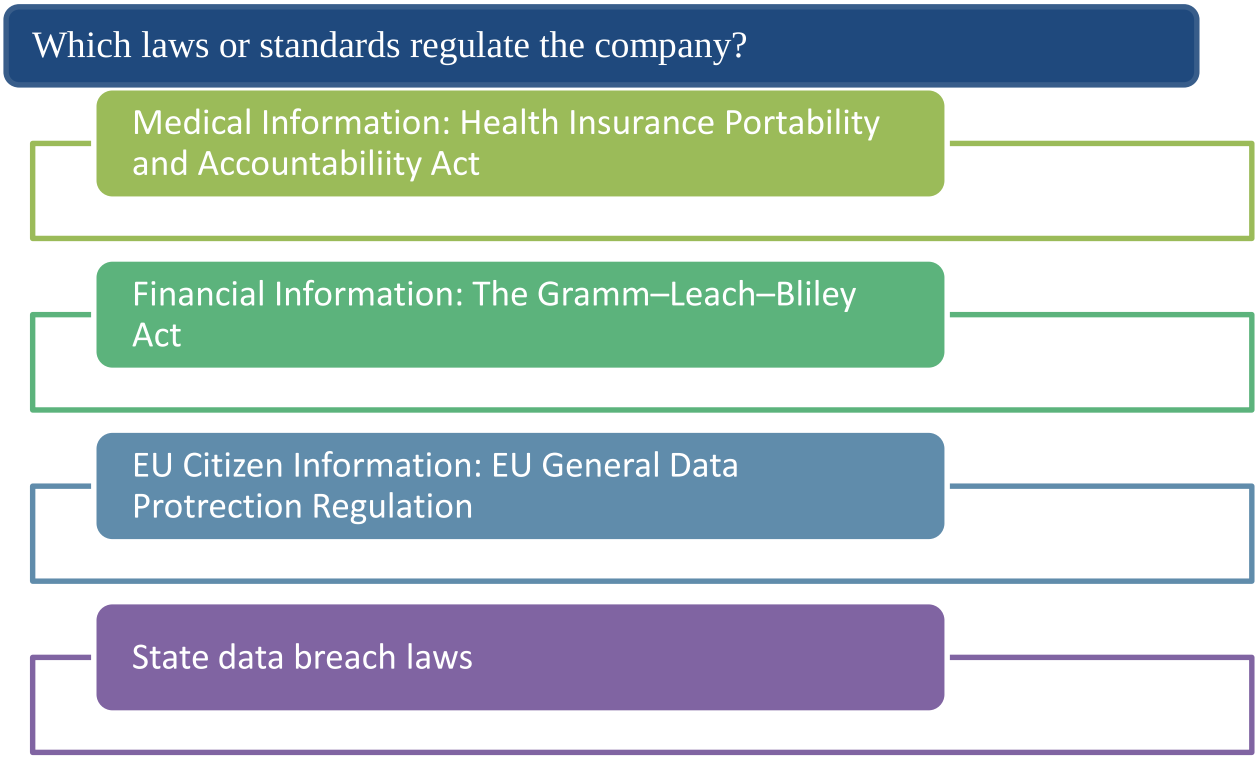
How Are Those Assets Protected?

Organization

How Does IT Report To The Board?

Is There Adequate Time On The Board Agenda?

Legal implications of cyber risks: The Board should understand the **legal implications** of cyber risks as they relate to the company's specific circumstances.



Which laws or standards regulate the company?

- Medical Information: Health Insurance Portability and Accountabiliity Act
- Financial Information: The Gramm–Leach–Bliley Act
- EU Citizen Information: EU General Data Protrection Regulation
- State data breach laws

Expertise and Adequate Resources: The Board should have adequate access to cybersecurity expertise and give cyber risk management regular and adequate time on Board meeting agendas. The Board should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

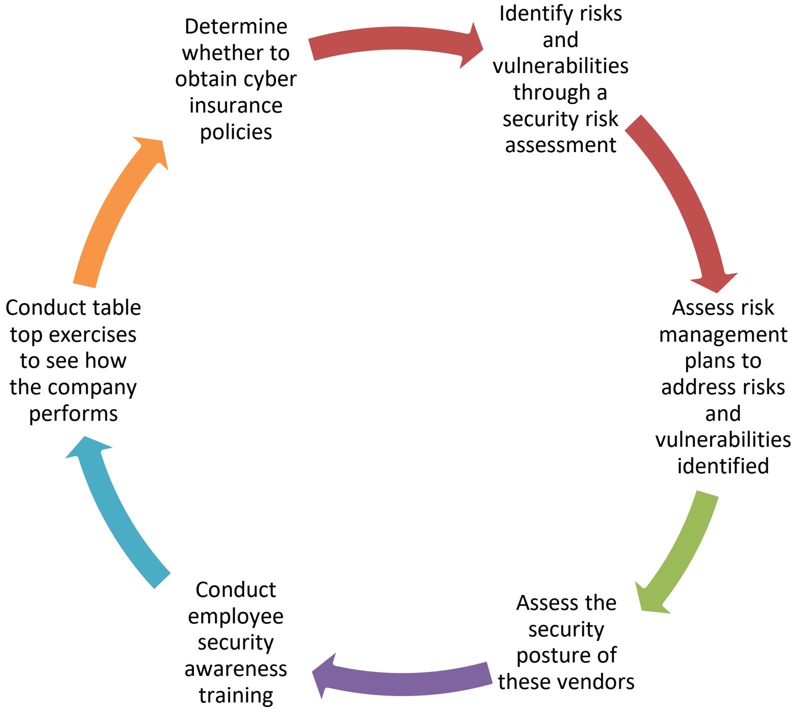
The Stop.Think.Connect.™ campaign has an online Resource Guide specific to SMBs. The guide contains information from SMBs on mobile safety information, cybersecurity guidance for employees, and a small business tip card, among many other resources. The Resource Guide for Small Business can be found here: http://www.stcguide.com/explore/small-business/

Small Business Administration (SBA) Training. This 30 minute, self-paced training exercise provides an introduction to securing information in small businesses. More information and the training can be found here: https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

The Federal Small Biz Cyber Planner tool helps businesses create custom cybersecurity plans. The Small Biz Cyber Planner includes information on cyber insurance, advanced spyware, and how to install protective software. More information can be found here: http://www.fcc.gov/cyberplanner

The Internet Essentials for Business 2.0 guide for business owners, managers, and employees focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs. More information about this guide can be found here: https://www.uschamber.com/internet-security-essentials-business-20

Managing risks: Management discussions should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance.


Identify risks and vulnerabilities through a security risk assessment
Assess risk management plans to address risks and vulnerabilities identified
Assess the security posture of these vendors
Conduct employee security awareness training
Conduct table top exercises to see how the company performs
Determine whether to obtain cyber insurance policies