CYBERSECURITY

SDDco Group

Evolving Threats Are Real.
Armor Your Network Against Vulnerabilities Before It's Too Late.

www.sddco.com | info@sddco.com | (212) 751-4422

CYBERSECURITY

Many companies spend a lot of money, time and effort securing their internal systems in hopes to avoid making headlines due to a security breach. A hacker can usually find a gap on which to capitalize and gain access to a firm's network, which is why conducting regular testing in an attempt to compromise your network is the best security reinforcement tactic. Is your protection sufficient enough to stop a real attack?

Cybersecurity has long been a concern for the SEC and FINRA. Firms of all sizes are now starting to think more along the lines of, "Could a security breach happen to MY business?"

We find although most firms have taken important steps to secure their networks, they often do not have a full protection suite of tools, which leave vulnerabilities wide open for hackers. Let's examine five cybersecurity myths that have been discredited.

Let's explore some common myths that many believe provides adequate protection for securing their network.

MYTH	FACTS	MYTH BUSTED!
#1 - We have a firewall and use antivirus software	• Antivirus software and a network firewall provides basic risk mitigation • They are not a comprehensive solution to protecting your firm • The greatest risk is a phishing attack, from which antivirus programs offer almost no protection • Firewalls left open pose vulnerabilities for penetration	Antivirus software and a firewall are important elements of your overall strategy, but they are not enough. With routine updates and maintenance, they must be complimentary parts of a bigger cyber strategy.
# 2 - Our IT service provider (SP) has addressed the SEC and FINRA's Cybersecurity Guidance	• IT and compliance professionals don't speak the same language • SEC Guidance: Firms must produce a Written Information Security Policy (WISP) and provide evidence that all firm employees understand and are following these policies • SEC recommends: Firms need Governance and a Risk Assessment, Access Rights and Controls, Data Loss Prevention, Vendor Management, Training, and Incident Response • FINRA Guidance – must provide WSP and bring in compliance with Regulation S-P (17 CFR §248.30), Regulation S-ID (17 CFR §248.201-202), The Securities Exchange Act of 1934 (17 CFR §240.17a-4(f) • FINRA recommends: technology governance, system change management, risk assessments, technical controls, incident response, vendor management, data loss prevention, and staff training • While SPs are an important part of your cyber compliance plan, they only address some Access Rights and Controls and Data Loss Prevention subgroups.	SPs speak in terms of network security and endpoint management; compliance officers often lack the technical expertise to advise on such details. Risk assessments recommended by the SEC and FINRA cannot be performed by the same entity that maintains your network. The assessments must be performed by an independent 3rd party to ensure unbiased results.

CYBERSECURITY

MYTH	FACTS	MYTH BUSTED!
#3 - Our business is too small to be a target	• Financial Services which is one of the top 3 industries targeted by hackers. • Small businesses tend to be less likely to have invested in cybersecurity protection which also makes you an easier target • Hackers are getting more creative by the day, now using bots and artificial intelligence to uncover vulnerabilities. This means that no one is resistant.	A small business is the perfect target for a hacker as you have a model that is quite attractive to them.
#4 - We only access secure portals or put everything on the cloud; our devices don't need protection	• Devices can be infected via a USB drive, email attachment, website, or an unsecured WiFi network • Once infected, devices can then transmit key strokes and login credentials that allow hackers to access your data in a secured portal • Many Cloud based applications keep a copy of your data to give you access when you are offline. That information can be used to impersonate you for fraudulent purposes, as well as to phish your contacts, among other things.	Smartphones, tablets, laptops, and desktops all need to be encrypted, monitored, and protected with an antivirus and mobile device management software.
#5 - We don't need cyber insurance	• Purchasing a cyber insurance policy is not equal to securing sensitive information. • Most traditional commercial liability policies do not cover cyber risks like property damage, personal and advertising injury claims arising from access, or disclosure of confidential information.	Take the time to talk to a cyber insurer. The time to find out about gaps in coverage is not after you have had a breach.[1]

We, as part of a compliance solution, test people on policy and procedure awareness, their endpoint security status, network vulnerabilities to external threats, and phishing simulations with our proven incident response management for all aspects.

SDDco Cyber's Compliance And Guidance Offering:

- **Become compliant with all state and federal requirements including FINRA, SEC, etc.**
- **Infrastructure Testing including Penetration Testing**
- **Customized and Tested Policies and Procedures**
- **Fully Managed Incident Response Coverage**
- **Data Security Training**
- **Vendor Due Diligence**
- **Risk Assessments**

We Do the Heavy Lifting for You. Armor Your Firm from Hackers and Threats Now!
It's Time to Leverage the Power of SDDco Cyber.

[1] Bentley Long, https://www.linkedin.com/pulse/five-ria-cybersecurity-myths-busted-bentley-long

SDDco
Group Offices

NEW YORK (Headquarters)

485 MADISON AVENUE
FLOOR 15
NEW YORK, NY 10022
(212) 751-4422

MIAMI

78 SW 7th St.
MIAMI, FL 33130

BOSTON

WeWork
ONE LINCOLN STREET
BOSTON, MA 02110
(617) 217-2641

www.sddco.com