What are Your Cybersecurity Strengths and Weaknesses?

Cybersecurity is a growing concern for the finance industry as cyberthreats continue to evolve. Because they house highly-confidential data, there is increasing pressure on firms to prove they have the right measures in place to protect against a breach.

The Securities and Exchange Commission (SEC) **recently released a report** that examined 75 finance firms registered with the SEC, including broker-dealers, investment advisers and investment companies ("funds"). Using 6 key questions, this infographic uses findings from the report to help you assess your own cybersecurity preparedness.

6 KEY QUESTIONS

01 Who is responsible for cybersecurity within your firm?

A majority of the examined firms maintain cybersecurity organizational charts and/or identified and described cybersecurity roles and responsibilities within the workforce.

Recommendation: It's important to know who's in charge of cybersecurity initiatives at your firm, but you should also be documenting and updating this information on a regular basis in order to meet compliance requirements.

02 How well do you vet your vendors?

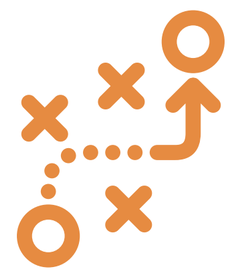
Almost all of the examined firms either conducted vendor risk assessments or required that vendors provide them with risk management and performance reports. Over half of the firms also required annual updates.

Recommendation: Third-party service vendors act as an extension of your firm. When evaluating third-party vendors, it's important to ensure that their cybersecurity posture matches yours.

03 What is your incident response plan?

Nearly all the examined firms had incident response plans in place, but less than two-thirds maintained them.

Recommendation: Plan maintenance is how firms can prove their commitment to cybersecurity preparedness. By having a plan in place, most of the work is already done. If your current plan is not being maintained, you should consider it a priority.



04 How do you educate your firm's employees?

Many of the examined firms required all employees to complete cybersecurity awareness training, but there was no way to ensure that proper training had happened.

Recommendation: Cybersecurity training for employees should be mandatory—not just as part of new-employee orientation, but as an ongoing practice. Plus, it's important that training is delivered in an engaging and memorable way so employees are more likely to retain the information.

05 What are your vulnerability assessment and penetration testing methodologies?

Most of the examined firms conducted penetration tests and vulnerability scans on systems they considered critical. However, a number of firms did not fully remediate all of the high-risk vulnerabilities that these tests discovered.

Recommendation: Vulnerabilities should be addressed immediately to reduce the risk to your network. If you know there are gaps in your security measures, then it's very possible cybercriminals know about them too.

06 How are you meeting your industry's regulations and compliance obligations?

Most of the examined firms had policies and procedures in place to meet SEC regulatory requirements. However, some firms were not adequately conducting system maintenance, such as the installation of software patches to address security vulnerabilities.

Recommendation: It's important to understand what is required of your firm and show that you're actively taking measures to prepare for additional compliance obligations. And always practice good patch hygiene. The WannaCry ransomware strain that spread earlier this year is a great example of why patches must be completed as they come available, not as areactive measure.

Cybersecurity preparedness is an ongoing commitment that requires firms to:

Continually assess and re-evaluate policies and know what cyberthreats are trending.

Keep track of the compliance regulations in their industry and how they are evolving.

Hire the right people and train employees on cybersecurity best practices.

Constantly test their own network and act on vulnerabilities.

We Can Help.

The firms in this report have taken critical steps to protect their network and prepare for a cyberattack. But the job is never done. All organizations – regardless of their industry – should be constantly evolving their cybersecurity practices to stay current. It's the firms that fall behind that are most susceptible to attack.

eSentire Managed Detection and Response™ keeps organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Our 24x7 team of elite security analysts handle everything from forensic investigation to incident response, so you can focus on your clients – not on cybersecurity.

Learn more at **www.eSentire.com** or contact us to see how eSentire Managed Detection and Response can help protect your firm from threats.

esentire®

www.eSentire.com