Cybersecurity Vulnerability Response Plan

OVERVIEW

Cyber vulnerabilities have become increasingly prevalent and significant as criminals seek to exploit vulnerabilities to breach a company's information technology (IT) security defenses. Conducting a preliminary investigation of possible exposure to these vulnerabilities as they arise can help financial regulators evaluate the operational resiliency of their groups/domestic insurance companies and determine whether a cyber event has occurred that would require further investigation.

However, it is important to note that reported vulnerabilities do not necessarily indicate a cybersecurity breach that would trigger formal notifications and consumer protection requirements, as companies should be addressing vulnerabilities before they can be exploited. As such, many states assign the responsibility for investigation of significant reported vulnerabilities to financial analysis inquiry

ulnerabilities include the Microsoft Exchange
execution vulnerability and the Qualys cloud
ats to the company's internal systems as well
y access to, company confidential data.

xaminers and/or analysts through the ad-hoc
exposure or vulnerability has been identified
nations. It is, however, up to those examiners
when deciding to undertake such inquiries.

onal investigation, which could include calling
nd/or follow-up on recommendations by the
warranted, examiners should consult Exhibit C
on Examiners Handbook to identify relevant

the domestic lead state determines that a
on the breach should be promptly shared with
ates in accordance with existing regulatory
dbook can then be used in situations where a
breach checklist in Addendum A to
20 General Examination Standards.

Terms & Definitions

Investigations related to significant vulnerabilities are typically viewed as following up on financial exam work to assess IT security controls. As such, it is recommended that financial regulators take the lead in addressing

appropriate steps to

e. Has the insurance company taken steps to investigate its systems and logs for exploitation, persistence, or evidence of lateral movement? If so, has the insurance company remediated any identified exploitation or persistence and investigated its environment for indications of lateral movement?

See Exhibit C DSS 05.07

3. For vulnerabilities derived from breaches at insurer third parties:
   a. Was company data exposed, or does the third party have easy access to your data?
   b. Has access been restricted?
   c. What steps have been taken to mitigate the risk that your data was exposed?
   d. What communication has taken place?
   e. Has the insurance company addressed this issue with its third-party service providers, if applicable?

See Exhibit C ITPQ Question #3

Conclusions & Next Steps

Additional Resources

Cyber Alerts & Bulletins: