Financial Services - Executive Reporting

NOPSEC

Keeping Boards and Directors up to speed on Cyber-Security Issues

Slow on Reporting - Late to Action

Cybersecurity issues have moved front and center for boards of directors of all industries as the threat of a breach and subsequent effects are of paramount concern. Boards need solid, timely information to make the risk vs. reward calculations that are inherent in modern business planning and operations.

Targets of Choice

The financial services industry is no exception, being one of the prime targets of cybercriminals[1], as both industry executors and regulators have long been aware. But reports on the status of a firm's cybersecurity risks have been slow in coming. In 2015, the Federal Financial Institutions Examination Council released a Cybersecurity Assessment Tool (CAT) as a way of helping institutions assess their risk profiles and ability to counteract those risks through such means as threat intelligence, cyber security controls, and resiliency measures.

The Need for Quicker Responses, by Regulation

Cybersecurity teams advising their boards face need to:

- Stay abreast of the risks and threats their institutions face minute by minute.
- Provide meaningful information about the context of those risks so boards can make strategic decisions.

Testing & Assessment: A Three-fold Problem

1. Because they don't measure risk vs. reward, leadership may inadvertently encourage financial institutions to avoid risks altogether rather than taking reasonable ones. For example, mobile banking is inherently risky, but those slow to offer it lost out to those financial institutions that responded to their customers' preference for a bank-by-phone option.
2. Because these tests are usually cumbersome manual processes, they're undertaken perhaps once or twice a year, failing to keep up to date with ever-changing risks and threats.
3. There's no attempt to measure the ROI on cybersecurity investments, which makes it impossible for boards to decide whether their budgets are sufficient to defend their institutions.

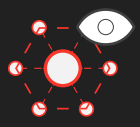
$1.5M The amount a mortgage lender was fined by the New York State Department of Financial Services in 2021, in part for failing to report a breach within the 72 hours of detection.

- Fully disclose all information of regulatory significance.
- Do all of this in a way that is coherent, manageable and consistent.

The Solution: A unified view of Institutional Risk, Response Options and Analysis

NopSec's Unified VRM gives financial institutions and their leadership the comprehensive, timely and quantifiable information needed to manage vulnerabilities throughout their infrastructure.

1. Monitoring



Continuously observes a variety of hybrid environments externally and distributed ecosystems for potential entry points

2. Asset Discovery

Discovers and maps unknown external-facing assets and systems to the organization that may be connected to the corporate network

3. Analysis

Evaluates and analyzes asset attributes to determine if an asset is risky, vulnerable, or behaving abnormally outside of the baseline

4. Prioritization

Prioritizes risks and vulnerabilities and provides alerts based on prioritization analytics

5. Remediation

Provides automated action plans on the mitigation of prioritized threats with embedded native detection and response capabilities

Easy-to-use information is only possible when a platform is fully integrated into an institution's internal structure, as well as focused on external connections that may pose threats. UVRM provides this information as the final step of its process for safeguarding organizations. Before generating the report, the NopSec platform works through these 5 preliminary stages.

In this final phase NopSec's UVRM details benchmark progress, quantifying risk remediation and articulating risk to upper management for birds eye view of cybersecurity performance and ROI. Security postures can be viewed by region, business unit, product or other disaggregated measures. Top leadership can see organization performance by categories such as these:

Reporting

Comprehensively measures the health of the financial institution's security program

In today's environment, such information is not a luxury, it's a necessity. To learn more about how you can provide your board the information needed to make strategic decisions on security matters, contact us or schedule a demo.