USE CASE

Securing Financial Institutions

BACKGROUND

From Open Banking and Cloud Computing To Tomorrow's Innovations—Security Is the Foundation

The financial services industry is undergoing dramatic change. Open banking is revolutionizing the industry with an ever-increasing number of highly personalized and advanced services provided by third-party applications. Many assets are now cloud-based. Banking is conducted anywhere, anytime, from the palm of the customer's hand. As a result, maintaining security and trust has never been more complex, nor has it been more important.

Regulators Are Increasing Their Demands

Regulators are increasing their scrutiny of financial security practices, so risks and critical vulnerabilities require rapid reporting and transparency. Failure to comply with regulator demands can lead to significant fines and cause reputational damage. Therefore, it's imperative to quickly identify, remediate and report critical risks.

Auditors and Risk Managers Need Prompt Answers

The demands of maintaining compliance with multiple local, regional and global standards drains your time, and can overwhelm your team with more internal compliance requests than they can accommodate. A unified dashboard is needed to quickly assess and measure vulnerabilities across the organization, and deliver the risk metrics and data you need to respond quickly and confidently.

Legacy Vulnerability Management Doesn't Help

Legacy vulnerability management (VM) tools weren't designed to handle the modern attack surface and its growing number of threats. Their visibility is limited to traditional IT assets, missing any vulnerabilities present in cloud, operational technology (OT) or container environments.

Legacy VM tools are also risk-unaware, relying exclusively on Common Vulnerability Scoring System (CVSS) base scores to determine which vulnerabilities to remediate. Since CVSS base scores are static and lack any degree of business context or threat intelligence, they can lead security teams to waste the majority of their time chasing after the wrong issues while missing many of the most critical vulnerabilities that pose the greatest risk to the business.

Data Points

- Financial services remains among the top targeted sectors for cybercriminals[1]
- 91% of financial services attacks are financially motivated
- 63% of attacks are perpetrated by external attackers
- 18% are financially motivated insider threats

Recent Events

- **March 2020**: Kryptik trojan accounts for over 70% of threats affecting financial services
- **February 2020**: Hackers target PayPal's Google Pay integration to make tens of thousands of dollars of unauthorized purchases
- **December 2019**: Sodinokibi ransomware takes down Travelex computer systems and demand $6 million to remove it
- **November 2019**: Emotet botnet re-emerges as a serious threat, affecting financial institutions worldwide

[1] Verizon, "2020 Data Brief Investigations Report"

Key Challenges

- Financial services have dynamic, heterogeneous, global networks with internet-facing assets that are exposed to attack
- Regulators, auditors and risk managers scrutinize security with new demands for rapid identification and reporting of critical risks, under threat of severe fines
- Customer expectations of continuous availability make it difficult to take the system down for updates and maintenance needs
- Large geographically distributed organizations create a large attack surface with numerous attack vectors
- IT teams are overwhelmed with requests and need to know what really matters
- Third-party applications and innovations, like "open banking," increase security risks

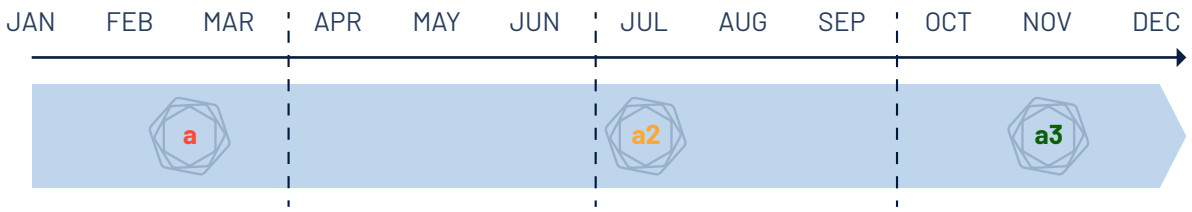
Add Value, Not Blind Capacity Building

In times of crisis and change, reducing costs and improving efficiency is critical. Add value to the business by focusing first on what matters most. Prioritize effectively to save time and money and not just deploy costly new controls.

The Maturity-Based Security Approach: Outdated and Ineffective

In a 2019 study, McKinsey stated that maturity-based capacity building "can never be more than a proxy for actually measuring, managing, and reducing risk."[2] This is because maturity-based security strategies are a recipe for cost overruns and excessive growth. Financial services, IT and security professionals need to focus on building value by reducing risk, not just blindly building capacity.

The Red-Amber-Green, or "RAG", score approach is a critical mistake made by many financial institutions. In the RAG methodology, a generic risk is identified and labeled as "red." Once a control is fully deployed, the risk label is changed to "green" and the risk is reported as controlled. Unfortunately, heat maps and RAG charts are not effective. Even worse, such reports are often based on guesses.



With a risk-based approach, you can prioritize security investments based on effectiveness in reducing risk —not just capacity-building milestones. This helps security leaders maximize the impact of their existing resources and show quantifiable value to business leaders.

[2] McKinsey & Co., "The Risk-Based Approach to Cybersecurity," October 8, 2019

“SIMPLY REORDERING SECURITY INITIATIVES... ACCORDING TO THE RISK-BASED APPROACH INCREASED PROJECTED RISK REDUCTION 7.5 TIMES ABOVE THE ORIGINAL PROGRAM AT NO ADDED COST”

— McKinsey on Risk[2]

Accelerate IT Response by Prioritizing What Matters Most

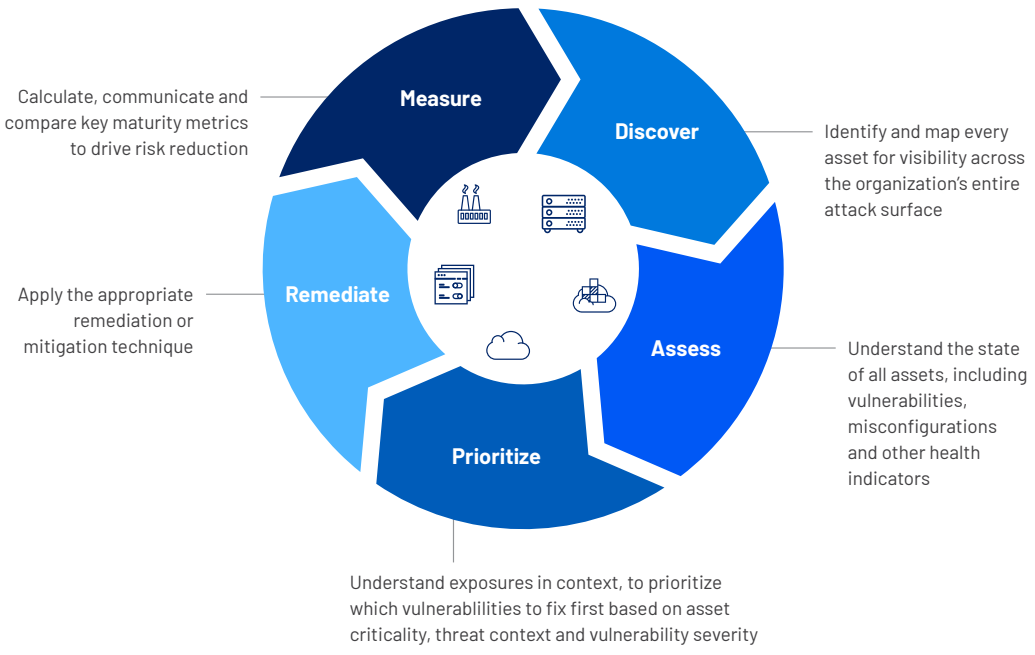
Many security teams prioritize every vulnerability with a CVSS base score of 7.0 and above. But more than half of all vulnerabilities fall into this category. You will never have enough time or resources to mitigate all of these vulnerabilities, and IT teams can quickly become overwhelmed—and annoyed. For financial institutions adhering to PCI DSS standards, which call for remediation of every vulnerability with a CVSS base score of 4.0 and above — roughly 94 percent of all vulnerabilities — the overload problem is even worse. In either case, CVSS-based prioritization causes workloads to quickly spiral out of control.

If you’re using CVSS to prioritize, you almost certainly have more vulnerabilities than your security and IT teams can manage. And with a well-funded, highly-skilled, motivated group of adversaries, you can’t afford to waste time on vulnerabilities that don’t pose real business risk. Partner with your IT team and encourage rapid remediation by prioritizing the relatively few vulnerabilities that pose the greatest risk to your most critical assets.

Evolving to a risk-based VM strategy is a far more comprehensive solution than you can get while using legacy VM tools. Rather than just discovering and assessing vulnerabilities, you’ll be able to effectively prioritize them, determine the appropriate action to take and calculate key metrics as well as compare against industry standards. This approach not only helps you determine when and where to make adjustments to optimize your strategy, but it enables you to build and maintain management’s confidence and keep them out of panic mode when high-profile exploits occur.

By reducing workloads and focusing first on the risks that matter most, you can evolve from a highly reactive program, which is interrupt- driven and error-prone, to one that is more proactive and strategic, so you can maximize your efficiency and effectiveness.

Lifecycle for Risk-Based Vulnerability Management



Quickly Answer Regulators, Audit and Risk Managers with Confidence

A risk-based approach, with vision of the entire attack surface and quantifiable cyber risk metrics, also provides the information you need to quickly and confidently respond to oversight demands. No matter which regulatory agency your organization answers to, compliance requests likely consume a large amount of your team's time, and failure to quickly answer a compliance request can cause massive fines and problems. Once you have established a clear approach to understanding and managing your cyber risk, these concepts are easily visualized and communicated to internal and external stakeholders.

Compliance Doesn't Equal Security

Remember that passing an audit is not the same thing as maintaining a high level of security. First, most compliance regulations are written to protect consumers, not to safeguard your business. As a result, you can pass every audit easily, yet still not be secure. However, if you achieve and maintain a high level of security, you're highly likely to pass that portion of your audit as well.

Regulatory audits also only consider a subset of your assets to be in-scope, so focusing exclusively on those can lead you to ignore other business-critical assets and the vulnerabilities that reside on them. In addition, focusing on regulatory compliance often leads to point-in-time assessments at irregular intervals.

Summary

As a cybersecurity professional in financial services, you know that your network is a primary target for well-funded, highly skilled, highly motivated cybercriminals. And you also know that each new service the business develops creates additional attack vectors for these adversaries. You need to cut through the noise and focus on the vulnerabilities that pose the most risk. Risk-based VM enables you to focus on what matters most, so you can make the best use of your limited resources and stay ahead of adversaries.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.