

Banking on Cyber Integrity

Prepare to Grow Past \$10 Billion with Tripwire and Tevera

Unfortunately, the risks and costs of cyberattacks appear to be growing. And the consequences of such attacks could have devastating and long-lasting collateral effects. Cybercriminals are only becoming more cunning and sophisticated. It is estimated that cybercrime will cost businesses approximately \$6 trillion per year on average through 2021.

— U.S. Securities and Exchange Commission

Building customer trust is paramount to the success of any company, but perhaps nowhere more so than in the banking industry. Cyberattack strategies are increasingly innovative, putting pressure on banks to protect their data or make the headlines when the next big breach takes place. The Bangladesh cyber heist of 2016 is one infamous example of threat actors' ingenuity: Hackers used malware to steal \$101 million¹ through the SWIFT international transactions network at the Federal Reserve Bank of New York.

This urgency to tighten cybersecurity doesn't just come from internal stakeholders, either. Once banks reach \$10 billion in assets, several complex regulatory demands take effect. How growing banks perform in this pivotal phase can make or break their long-term success. Underprepared banks that fail stress tests requirements, for example, face fines and significant business setbacks.

According to BNY Mellon's² 2017 Annual Report, "The failure to maintain an adequate technology infrastructure with effective cybersecurity controls

relative to the type, size and complexity of operations... could impact operations and impede our productivity and growth, which could cause our earnings to decline or could impact our ability to comply with regulatory obligations leading to regulatory fines and sanctions."

When the \$10 billion threshold appears on the horizon, banks must begin preparations immediately with the help of industry experts like Tevera and Tripwire. Help your board of directors demonstrate active risk mitigation and meet expectations from regulatory bodies like the Federal Deposit

Insurance Corporation (FDIC). It's never too early to begin putting foundational cybersecurity controls in place.

What \$10 Billion Means for Banks

It can take years for banks to adequately prepare for the security and compliance realities that set in when banks reach \$10 billion in assets. Strategically planning and executing a strategy is essential to withstanding the demands of stress testing and meeting regulatory compliance. Other considerations that become more pressing as banks grow are the Volcker Rule of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Consumer Financial Protection Bureau fines, and fees from the Durbin Amendment.











Dodd-Frank Act Stress Testing

The Dodd-Frank Wall Street Reform and Consumer Protection Act requires that banks with \$10–50 billion in assets conduct annual stress tests, known as DFAST (Dodd-Frank Act Stress Testing). Stress testing involves risk assessment for baseline, adverse and severe conditions in the financial market—requiring substantial resource use and detailed data logging. Results must be shared with the FDIC and ultimately published.

In addition to DFAST, the Dodd-Frank Act instituted the Consumer Financial Protection Bureau to ensure fair and transparent practices at banks over the \$10 billion mark. Yet another component of the Dodd-Frank Act also kicks in at this milestone: the Volcker Rule, which prohibits certain types of proprietary trading.

Regulatory Compliance

As the banking industry is heavily regulated, continued growth depends upon compliance with standards like GLBA, SOX, FFIEC, SWIFT, COBIT, SEC, and state and federal audits. The regulatory bodies overseeing banks require stringent security policy compliance be met. Banks must prove they have an effective change management process in place.

Control	Tripwire Coverage	Details
Network perimeter defense tools (e.g., border router and firewall) are used.		Tripwire® Enterprise can monitor perimeter defense tools like firewalls to ensure the configuration has not been modified.
Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.		Tripwire Enterprise rules and policies can be used to ensure local firewalls are enabled.
All ports are monitored.		Tripwire Whitelist Profiler can monitor ports and services and compares the current state against a tailored set of customer-specific approved port and services, alerting when monitoring detects a variance.
Up to date antivirus and anti-malware tools are used.		Tripwire Enterprise rules include tests for antivirus and can be created to monitor malware solutions as well.
Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced.		Tripwire Enterprise establishes and maintains consistent compliance agent-based and agentless continuous configuration assessment against over 800 combinations of platforms and security and compliance policies, standards, regulations and vendor guidelines.
Ports, functions, protocols and services are prohibited if no longer needed for business purposes.		Tripwire Whitelist Profiler enables you to define a set of required or permitted system settings. When a system is examined, a comprehensive report of authorized and unauthorized settings is generated along with the justification information.
Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.		Tripwire Enterprise checks across large heterogeneous environments to provide threat detection and instant insight into configuration vulnerabilities while increasing operational efficiency by reducing configuration drift and unauthorized change.
Programs that can override system, object, network, virtual machine, and application controls are restricted.		Tripwire Enterprise monitors the configuration of the system and Tripwire Log Center® monitors the logs.
System sessions are locked after a predefined period of inactivity and are terminated after predefined conditions are met.		Tripwire Enterprise policy tests can be used to ensure these controls are in place and applied consistently.
Wireless network environments require security settings with strong encryption for authentication and transmission.		Tripwire can test the security settings for compliance with internal or FFIEC policy.

The larger a bank becomes, the more important it is to deploy a solution robust enough to satisfy auditors. This means finding a security solution with baked in file integrity monitoring (FIM), security configuration management

(SCM), vulnerability management and log management. When banks leverage a tool that automates alerts on unauthorized changes and misconfigurations, it's much easier to prove compliance.

The FFIEC Maturity Model Baseline

The FFIEC (Federal Financial Institutions Examination Council) is an interagency body of federal banking regulators. Their baseline cybersecurity maturity requirement puts forth the foundational security practices banks must have in place. Beyond the baseline, they supply further recommendations for reaching evolving, intermediate, advanced and innovative cybersecurity maturity.

A bank's cybersecurity maturity level is determined by the FFIEC Cybersecurity Assessment Tool (CAT), which focuses on five specific domains:

- » Cyber risk management and oversight
- » Threat intelligence and collaboration
- » Cybersecurity controls
- » External dependency management
- » Cyber incident management and resilience

Use Tripwire Solutions to Align with the FFIEC

Each domain contains several criteria banks can use to reach a baseline or above maturity level. Security professionals responsible for compliance and audit success need the appropriate tools to accomplish this. When we look at the baseline cybersecurity controls requirements domain 3, for example, we can see how Tripwire solutions achieve each specific objective.

Proven Success

Tripwire is no stranger to the security needs of large, multinational banking institutions, with a track record of helping banks improve their IT security posture and align with regulatory requirements in the process. Tripwire's tightly-integrated capability suite helps financial institutions deliver reliable and secure services while withstand the stress testing necessary to facilitate their continued growth in the global financial market.

Organizations often have a build sheet or gold image but see considerable drift from that over time —and no way to analyze systems in real time for compliance related to system changes. Tripwire solutions help banking institutions remediate security vulnerabilities and compliance misconfigurations across their on-premise, hybrid and cloud environments.

The FIM and SCM capabilities of Tripwire Enterprise, for example, provide detailed reporting on unauthorized changes and misconfigurations. As soon as a change is detected, an automatic validation process kicks off to verify that this change did not take the system out of compliance or introduce new vulnerability risk. Tripwire solutions integrate with one another as well as with an extensive array of security products like Splunk.

Tevora Partnership

Tevora helps banks better understand and mitigate risks. They analyze banks' cybersecurity postures and map existing needs to Tripwire solutions. This aids banks in implementing the change and vulnerability management best practices that enable them to withstand the demands placed on them upon surpassing \$10 billion in assets.

In addition, Tevora focuses on evaluating, recommending and implementing security controls that protect server, network and endpoint infrastructure from advanced threats using the NIST Cybersecurity Framework as a baseline for evaluating the effectiveness of a control. Tripwire Policy Manager establishes and tracks alignment with this and other controls.

Summary

If your organization struggles to support "checking the box" for regulatory purposes or is focused on strengthening security controls in preparation for hitting the \$10 billion milestone, Tripwire can help. Tripwire supports FFIEC policy controls "out of the box" for a wide range of platform and device types.

About Tevora

Tevora is a management consultancy focused on cybersecurity, risk, and compliance services, supporting the CISO in securing their organization's digital assets. Tevora makes it their responsibility to ensure the CISO is equipped with the information, tools and guidance they need to build their departments so they can prevent and respond to daily threats and risks. Learn more at www.tevora.com.

Request a Demo

Let us take you through a demo of Tripwire Enterprise and answer any questions you have. Understand how Tripwire's suite of security and vulnerability management products and services can be customized to specific IT security and compliance needs. Visit tripwire.com/contact/request-demo to schedule your demo today.

1 https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

2 <https://www.bnymellon.com/us/en/investor-relations/annual-report-2017.jsp>



Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at tripwire.com**

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter [@TripwireInc](https://twitter.com/TripwireInc) » Watch us at youtube.com/TripwireInc