

Financial Services, UK Case Study

Confident IT Governance and Continuous Risk Assessment

Case Study Overview:

Learn how a global financial services firm more effectively manages IT security and compliance risk through actionable intelligence provided by Skybox View Suite.

Customer Profile:

- **Scope:** International
- **Business:** Investment banking, capital and equity markets, risk management.
- **Size and Assets:** Approximately 9,000 employees and £900 billion assets

Business Problem:

- Auditing network and application changes manually proved too time-consuming and problematic, as the number of changes each day exceeded 1,000—with roughly 100 of those having a direct impact on security posture and regulatory compliance effectiveness.
- While vulnerability scanners can create thousand-page reports listing various low, medium, and critical vulnerabilities, they provide no information about how much risk those vulnerabilities actually create for the organization. They present no context as to whether existing firewall policies, network segmentation, router configurations, and other security precautions effectively mitigated the risk. The firm needed a better way to focus on flaws and vulnerabilities that created real-world risk.

Solution:

Skybox View Suite:

- Skybox Secure – Vulnerability Lifecycle Management
- Skybox Assure – Network Security Compliance

Noteworthy Customer Quote

"Skybox lets us look at our environment in a very clear, risk-based fashion. With Skybox, I believe, we now are managing more based on fact."

"With Skybox, we can demonstrate to auditors that we're managing our processes. We can show them that we have preventive, detective, and reactive controls in place. If anything falls through the cracks, we can catch those slips."

"Skybox shows you that those low or medium-ranked vulnerabilities, that were previously ignored, are actually exposed to the Internet that could lead to the compromise of a back-end server. Skybox gives you the ability to see your vulnerabilities in the context of the controls in place. That's simply fantastic."

"Skybox has reduced the number of vulnerabilities we need to mitigate immediately to a manageable 1 percent."

Introduction

A leading financial services firm in the United Kingdom knows how to handle risk. With more than £924 billion in assets, and 9,000 employees operating in 26 countries, this investment bank has global reach. It provides financial services and risk management solutions needed by corporations, financial institutions, governments, and multinational organizations. The UK-based firm is constantly deploying new applications, updating its networks, and expanding rapidly around the globe. It possesses a world-class trading platform for faultless electronic services and automated execution for fixed income, futures, commodities, and equities markets.

Its regulatory pressures are as intense as they get. The firm must comply with 46 separate regulatory bodies throughout the world, including the U.S. Securities and Exchange Commission, the UK-based Financial Services Authority, and the Monetary Authority of Singapore. And the firm is rapidly growing – and this business expansion accelerates the risks associated with the firm's digital assets and infrastructure: applications deployed need to be secure and compliant; firewall and access control rules not only have to be secure, but changes to the system can't affect availability; and all-the-while newly announced software vulnerabilities mean the risks posed against its thousands of servers and PCs must be reevaluated constantly. *"That makes quite a challenging environment in terms of scale,"* says the firm's head of its information risk management team. The stakes are high in the world of investment banking: a single technological mistake could cost millions of dollars a minute, or failure to comply with regulations could result in fines and other hefty sanctions.

A Comprehensive Risk-Based Approach

To manage the company's regulatory and IT security risks, the executive and his team (six who report directly and 26 security managers) have taken a proactive approach to its security and compliance risk management programs. Wherever possible, they streamline the processes associated with vulnerability management and all of the business processes associated with internal risk management, governance, and instilling detective and preventive regulatory controls throughout their business technology systems. His team, in partnership with other technology teams, has cut the time required to patch its systems from weeks to less than four hours, drastically reducing the window of exposure to key applications. In addition, it has built a comprehensive regulatory records management system aimed at reducing the risks associated with regulatory-related fines.

Rather than relying on mandatory system governance and regulatory checklists to reach compliance, the information risk management team takes a comprehensive risk-based approach that encompasses their daily operations, and aligns risk with business goals, such as those called for by the Control Objectives for Information and related Technology, or COBIT, framework of best practices. This enables IT to maximize security effectiveness in the most cost-efficient and business-focused ways: a risk management program that is objectively measurable, practical, and focused on real-world business situations.

Two crucial aspects of its risk management program include the ability to efficiently manage application, network, and access control policy changes, as well as more effectively mitigate software vulnerabilities that arise almost daily.

The Business Problem Is Complex and Constantly Changing

For a global infrastructure as vast and complex as this financial services firm, with thousands of end-points, and hundreds of servers, it's an ongoing battle to identify, assess, test, and remedy every software vulnerability that arises. In fact, according to CERT, newly discovered vulnerabilities for 2006 (as of Oct) numbered 5,340. Clearly, 2006 will surpass the 5,990 vulnerabilities discovered during all of 2005, and significantly surpasses the 3,780 recorded for all of 2004. With nearly 140 new vulnerabilities announced each week, organizations – without the proper insight into how their network segments, firewall rule sets, and other existing security controls mitigate these risks – are forced to expend enormous efforts to rush and patch all of their systems immediately following the release of a software vendor's patch – a predicament that not only consumes precious operational resources, but is prone for errors.

In addition, the firm averages more than 1,000 system changes each day, with 100 of those modifications directly affecting its security and compliance risk posture. The complexity of the firm's systems and the velocity of change means mistakes can be made that could affect application availability and security. *"We recruit very bright people, and train them very well. But the problem that arises is that these people are very good at convincing everybody that the changes they're proposing are the correct changes."*

For these reasons, the firm sought a way to bring quantifiable insight into both its change control and vulnerability management processes. It needed to be able to quickly verify that application and network access control changes work as intended, and be able to consider the actual risks that software vulnerabilities impose when vetted against the firm's actual infrastructure and layered security defenses. But that would require a way to automatically and periodically discover, map, and model its global infrastructure, and attempting to do so manually would not only be impossible to keep up to date, but extraordinarily time consuming, with the risk of costly mistakes.

The Solution

To get the job done, the firm turned to Skybox Security Inc., which pioneered the science of risk quantification and advanced analytics applied to the challenge of IT risk assessment, compliance, and control optimization. Skybox's solution, Skybox View, is an integrated suite of Security Risk Management applications: Skybox Secure and Skybox Assure. Both are built on a modular, open, and scalable architecture that enable security and IT operations teams achieve an integrated and accurate view of their organization's risk and control compliance posture. Unique modeling, simulation, and what-if analysis technologies set Skybox apart from the traditional threat and risk assessment solutions.

Designed for the security team, Skybox Secure focuses on vulnerability lifecycle management as well as the automation of previously labor-intensive risk assessment and mitigation planning processes. With Skybox Secure,

organizations can reduce risk exposure, make better decisions, and generate precise and prioritized battle plans in minutes rather than days or weeks.

Whereas operations and other IT teams turn to Skybox Assure to automate their network security compliance and auditing processes. Organizations around the globe use Skybox Assure to conduct firewall audits, validate network policy compliance, compare control change impact, document historical changes, and generate comprehensive audit and compliance reports.

"You can't convince Skybox that a bad change is the right change. Skybox thoroughly examines the reality of your infrastructure, measures it, and presents it back to you with how a change, or a vulnerability, is affecting the level of risk you're actually exposed to," says the executive. "Even if everyone on your staff is convinced that a change is correct, or that a patch mitigated a vulnerability—and it in fact didn't—Skybox will catch what everyone thought was resolved, but in actuality wasn't."

Many companies operate by running vast vulnerability scans that generate reports thousands of pages long, only to focus on the critical vulnerabilities. *"They'll print a 10,000 page report and just throw away the back two-thirds," says the executive. "That's not the most effective way to manage risk. Skybox shows you that those mediums that were going to be ignored actually are exposed to the Internet, and could lead to the compromise of a back-end server. Skybox gives you the ability to see your vulnerabilities in the context of the controls in place. That's simply fantastic."*

Prior to Skybox View, every six months, the firm conducted time-consuming, manual reviews of its IT infrastructure and overall risk posture. Inability to fix the vulnerabilities in a timely manner guaranteed a minimum of six-months of exposure to newly announced vulnerabilities. Today, those reviews are fully automated, and run every evening. *"Skybox has reduced the number of vulnerabilities we need to mitigate immediately to a manageable 1 percent,"* the executive says. And by fixing those top vulnerabilities that matter to the environment, Skybox significantly reduces their window of risk.

As a result, IT teams are no longer pressured to deploy patches across all of their systems the very week, or day, they're disclosed. They can strategically focus on the few systems that pose the greatest risk – and roll the remaining patch updates into the organization's scheduled maintenance cycle. *"That's how Skybox not only helps us to reduce our risk, but to also focus the operational efforts that used to be directed at patching to more productive endeavors,"* the executive says.

Higher Confidence in Overall Compliance

Regulatory compliance requires that organizations keep their systems secure, and that they have verifiable network and application controls in place to ensure only those who are authorized can access regulated information. Skybox View enables this firm to automate many of the labor-intensive processes involved with compliance efforts, uncover policy violations, and optimize network controls. *"With Skybox, we can demonstrate to auditors that we're managing our processes. We can show them that we have preventive, detective, and reactive controls in place,"* he explains. *"If anything falls through*

the cracks, we can catch those slips. This lends to a much higher level of confidence in our posture," he says.

Thanks to the aid of Skybox, the firm now conducts more thorough and frequent analyses of its ongoing risk and compliance posture. With Skybox, the firm models its infrastructure, each day, through system threat profiles and information about the firm's network access information, vulnerability data, and classifications of IT assets. *"We can actually see how our environment is changing. We can see changes that didn't go through our formal change control process, and that could place us at risk. Most importantly, we can see how our overall level of risk is changing on a continuous basis."*

That's a powerful, organization-changing capability, and it's affected the firm in a few unpredictable ways. It's always been the security team's focus to build a cohesive partnership with other business units and IT operation groups—rather than the all-too-typical situation in which security units throw up operational walls and hurdles. *"Instead of just showing up and saying you have to stop all of your work and patch everything now—oftentimes with insufficient documentation to back up our assertions—we now can show other groups the two or three things they may have to fix right away. Skybox has proven to be one of the few tools that empower us to do that. Instead of just handing out problems, we now arrive with solutions. Instead of being scary, it's more of a warm glow."*

#

Editorial Note:

Skybox View® is an integrated family of Security Risk Management applications. A set of shared services for each Skybox View application is provided through a modular, scalable framework. These include modeling, analysis, simulation, visualization and workflow management. Today, the Skybox View supports two applications: Skybox Secure and Skybox Assure.

Skybox Secure™ is all about managing the lifecycle of vulnerabilities within the context of network controls and policies. With Skybox Secure, the security team receives a precise and prioritized risk battle plan, saves money through process automation, while management gains unprecedented visibility into the organization's risk and governance profile. The result is reduced risk, reduce IT workload while transforming security from a reactive and defensive practice to a true business enabler.

Skybox Assure™ is all about network security compliance. It is primarily deployed and managed by the IT operations team in order to audit control and policy effectiveness in context with risk exposures. With Skybox Assure, organizations can maximize control and access effectiveness while minimizing risk exposure. The result is reduced IT workload by transforming security control management from an error-prone process to an automated, reliable, and accurate process.