IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

IT Security

The Need for Effective Third-Party Risk Management in Financial Services

Tom Turner

Tom Turner
CEO and President
BitSight

Biography

Tom Turner is CEO and President of BitSight (https://www.bitsighttech.com). Tom has extensive security industry experience, and has helped build category-defining companies. Prior to joining BitSight, Tom was a founding member of the executive management team of IBM Security Systems, a new division within IBM Software group that was created on the heels of the Q1 Labs acquisition.

Formerly, he was Senior Vice President of Marketing and Channels at Q1 Labs, where he was responsible for all product management efforts, demand-generation programs, and channel sales and marketing initiatives. Before joining Q1 Labs, Tom served as Director of Marketing for endpoint security at Cisco Systems, where he helped elevate the company to the number two position in the host-based, IDS/IDP market.

Keywords Business risk, Risk intelligence, Third-party risk, Data breaches, Cyber security ratings, Vendor risk
Paper type Research

Abstract

Third-party cyberattacks against financial institutions are on the rise, with the Financial Conduct Authority (FCA) reporting an 80% increase last year. In this article the author describes the current risk landscape, with reference to the recent SWIFT cyberattacks, and explores strategies that organizations can utilize to manage risk.

Introduction

In the last few years we have seen the frequency and severity of third-party cyberattacks against global financial institutions continue to increase. One of the biggest reported attacks against financial organizations occurred in early 2016, when $81 million was taken from accounts at Bangladesh Bank.

Unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia. The Bangladesh Bank managed to halt $850 million in other transactions, and a typo made by the hackers raised suspicions that prevented them from stealing the full $1 billion they were after.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Landscape

The Financial Conduct Authority (FCA) reported 69 attacks in 2017 compared to 38 reported in 2016[1], a rise of more than 80% in the last year. We saw two main trends last year. First, there was a continuation of cyberattacks targeting systems running SWIFT – a fundamental part of the world's financial ecosystem.

As the SWIFT software is unified and used by almost all the major players in the financial market, attackers were able to use malware to manipulate applications responsible for cross-border transactions, making it possible to withdraw money from any financial organization in the world. Victims of these attacks included several banks in more than ten countries around the world.

Secondly, we saw the range of financial organizations that cybercriminals have been trying to penetrate expand significantly. Different cybercriminal groups attacked bank infrastructure, e-money systems, cryptocurrency exchanges and capital management funds. Their main goal was to withdraw very large sums of money.

With the evolving risk landscape and the challenges of new potential risks including third party risks, companies within financial services need a set of management procedures and a framework for identifying, assessing and mitigating the risks these challenges present. Effective risk management offers sound judgement in making decisions about what is the appropriate resource allocation to minimize and mitigate risk exposure.

Risk management lifecycle

The basic principle of a risk management lifecycle is to mitigate risk, transfer risk and accept/monitor risk. This involves identification, assessment, treatment, monitoring and reporting.

In order to 'mitigate risk', an organization must measure cyber risk performance and incentivize critical third-party vendors to address security issues through vendor collaboration.

In terms of 'identification', you cannot manage your risks if you don't know what they are, or if they exist. The first step is to uncover the risks and define them in a detailed, structured format. You need to identify the potential events that would most influence your ability to achieve your objectives, then define them and assign ownership.

Once the risks are identified they need to be examined in terms of likelihood and impact, also known as assessment. It is important to assess the probability of a risk, and its consequences. This will help identify which risks are priorities and require the most attention. You need to have some way of comparing risks relative to each other and deciding which are acceptable and which require further management. In this way you establish your organization's risk appetite.

To 'transfer risk', an organization is advised to influence vendors to purchase cyber insurance to transfer risk in the event of a cyber event.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Once the risk has been assessed, an approach for treatment of each risk must now be defined. After assessment, some risks may require no action, to only be continuously monitored, but those that are seen as not acceptable will require an action or mitigation plan to prevent, reduce, or transfer that risk.

To 'accept and monitor risk', the organization must understand potential security gaps and may need to accept certain risks due to business drivers or resource scarcity.

Once the risk is identified, assessed and a treatment process defined, it must be continuously monitored. Risk is evolutionary and can always change. The review process is essential for proactive risk management.

'Reporting' at each stage is a core part of driving decision-making in effective risk management. Therefore, the reporting framework should be defined at an early point in the risk management process, by focusing on report content, format and frequency of production.

Managing with risk transfer

Risk transfer is a strategy that enterprises are considering more and more. It mitigates potential risks and complies with cyber security standards. As cybercrime rises, an insurer's view of cybersecurity has changed from being a pure IT risk to one that requires board-level attention. Insurance is now viewed as fundamental in offsetting the effects of a cyberattack on a financial institution.

However, insurers will want to know that appropriate and audited measures are in place to prevent an attack in the first place and respond correctly when cybersecurity does fail. An organization's risk management responsibility now extends down the supply chain and insurers will want to know the organization's strategies to monitor and mitigate third party vendor risk.

Simplifying risk management and the transfer of risk can also be accomplished by measuring your organization's security rating. This is a similar approach to credit ratings for calculating risk. Ratings provide insight into the security posture of third parties as well as your own organization. The measurement of ratings offers cost saving, transparency, validation and governance to organizations willing to undertake this model.

The benefits of security ratings will be as critical as credit ratings and other factors considered in business partnership decisions in the very near future. The ratings model within risk management can help organizations collaborate and have productive data-driven conversations with regards to risk and security, where they may not have been able to previously.

Long term potential

This year we will see a continuation of third-party cyberattacks targeting systems running SWIFT, allowing attackers to use malware in financial institutions to

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

manipulate applications responsible for cross-border transactions across the world. Banks generally have more robust cyber defences than other sectors, because of the sensitive nature of their industry and to meet regulatory requirements.

However, once breached, financial services organizations' greatest fear is copycat attacks. This is where an effective risk management strategy can enable better cost management and risk visibility related to business operational activities. This leads to better management of market place, competitive and economic conditions, and increases leverage and consolidation of different risk management functions.

Reference	
1	https://www.fca.org.uk/news/speeches/building-cyber-resilience