Bottomline Technologies®

BEST PRACTICES GUIDE

Cyber Fraud & Risk Management

3 Ways for Banks to Win

The Raging Battle Against Cyber Fraud

Cyber Threats Gaining

More than 100 banks in 25 countries – including the U.S. – were infiltrated by a sophisticated attack that siphoned $1 billion, much of it through ATM fraud.[1] Using malware dubbed “Carbanak,” the cybercriminals managed to pull off what many consider to be the most successful cyber heist against the banking industry.

That attack exemplifies the growing number and sophistication of cyber threats banks face today. In instances like this where the perimeter is breached, activities of an external attacker look the same as a malicious insider. Suspicious activity reports (SARs) filing in the industry hit an all-time high in 2014,[2] but what’s more worrisome is that employees and managers committed 78% of occupational fraud.[3]

2.4 million suspicious activity reports (SARs) were filed by banks last year.[2]

The growing risk is multifaceted.

- Fraudsters are infiltrating banks with very sophisticated tactics that are much harder to detect with traditional security controls.
- Attacks are lasting longer, going unnoticed by security systems and personnel for months after the initial infiltration, with exposure compounding by the second.
- Banks are finding that existing cyber fraud detection tools and processes are not enough. Traditional methods alone simply are not keeping pace against today’s cyber criminals.

3 Ways for Banks to Win

Considering this threat-ridden landscape, there’s no doubt that the banking industry’s approach to protection against cyber fraud needs to evolve to keep pace. The answer may be found in a more holistic approach that includes the following three best practices.

1. Use a proactive model.

Traditional cyber fraud detection solutions generally do not recognize the whole spectrum of potentially risky behavior. They rely on reviewing changes in embedded system data – such as log files and databases – presenting a limited picture of user activity on a bank's network. Some of the most obvious signs of risk, such as out-of-character behavior and arbitrary interactions, are not detected. Most log files typically capture only actions that prompt recorded change in data (i.e., addition or deletion) but not actions that include accessing and/or copying information without an actual change to the underlying data.

5–8 Months to Detect Fraud

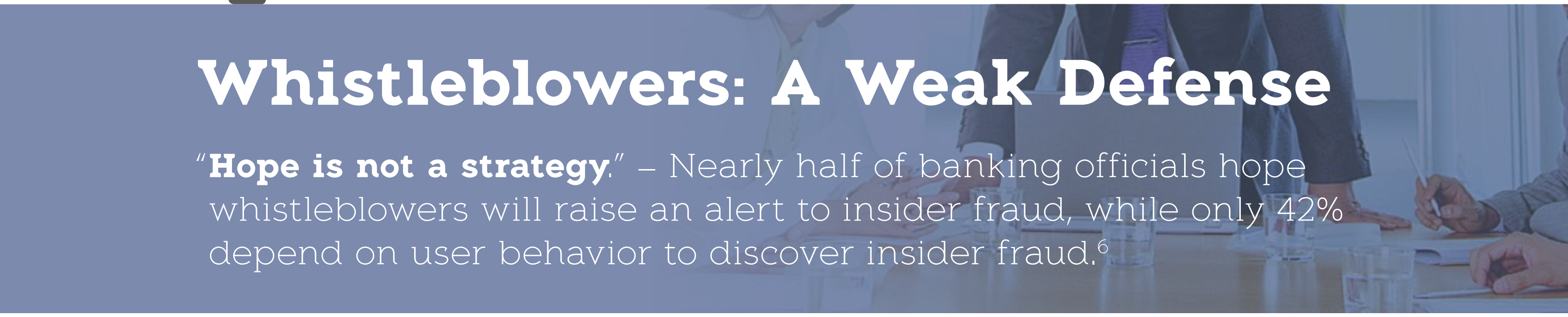
On average, it takes financial businesses 170 days to discover a malicious event, and 259 days when the attacker is an insider who has authorized access.[4]

Even if a system is in place to meet the FFIEC requirements[5] related to online banking, most systems lack an actionable warning for insider activity and user interactions with other core banking applications. Combing through the disparate data returned by a legacy system to find a red flag is both a financial and IT resource drain and causes delayed resolution. This is relevant not just to detect external bad actors, but also to minimize problems caused by authorized users unintentionally or intentionally introducing risk into the system.

Finally, older solutions are designed for *reactive* protection plans, and the nature of today's threats call for *proactive* diligence. While legacy security solutions are necessary, without a powerfully proactive capability in its cyber fraud detection arsenal, a bank is at best tolerating inefficiency and at worse under attack constantly without realizing it.

2. Monitor across external channels and internal functions.

Another challenge with static solutions: They haven't kept up with the digitization of internal processes and customer interactions. They just aren't flexible enough to handle the variety of technologies that are now part of today's banking infrastructure. This touches both external and internal activity.



Whistleblowers: A Weak Defense

"**Hope is not a strategy**." – Nearly half of banking officials hope whistleblowers will raise an alert to insider fraud, while only 42% depend on user behavior to discover insider fraud.[6]

Externally, customers can now use websites, mobile apps, e-checks, online transfers, etc. – in addition to ATMs and in-person visits – to do their banking. This multi-channel approach has brought multiple benefits to banking, but it has also increased security needs. First, there is more activity in general to monitor. Second, each channel has specific security needs, but there's also a need to evaluate overlapping behavior to model a holistic view of user behavior.

The same goes for internal users. They are using more digital solutions to do their work, and although this has increased productivity and collaboration, it has also created more separation. Islands of business platforms and data stores exist across functions and silos, and they must be monitored holistically to detect patterns that point to potential problems.

3. Build in efficiency to improve effectiveness.

Newer, more intelligent solutions simply are more efficient and effective than traditional ones and offer banks an opportunity to streamline operations as they enhance security.

Reducing the number of false alerts is a good example. Banks need the ability to efficiently capture, analyze, correlate, and develop user profiles to generate the right alerts – while keeping the false-positive rate low. They also need the ability to efficiently and thoroughly investigate suspicious activity while managing many cases at a time.

$3.7 trillion 2014 global insider fraud loss[3]

An effective solution for these needs should include a “self-learning” analytics engine that not only generates increasingly more accurate alerts, but also develops and applies a risk score to unusual actors to deliver real-time, dynamic profiling. That’s why a bank’s overall fraud solution should not only detect suspicious activity, but also provide management with the visibility and workflows needed to quickly identify which SARs should generate cases – and then efficiently execute the filings.

The driving technology is data visualization and link analysis, which can speed up investigations while providing a well-documented audit trial that can be used to build cases and demonstrate responsibility. The result is more accurate and informative outcomes without resource strain.

Get Ahead with These 3 Winning Practices

Is the Carbanak attack an anomaly or is it a precursor to the next generation of cyber fraud and threats against the banking industry? Considering that cyber fraud and cyber crime are expected to increase,[7] it is difficult to think that Carbanak is a once-in-a-lifetime incident. More realistically, it will soon be outdone by an even more sophisticated threat.

With the average annualized cost of cybercrime in the financial services industry $20.8 million,[8] no one in the banking industry can wait and wonder if their security and fraud prevention solutions could detect and stop another Carbanak. Instead, by applying these three best practices to gain better insight into user behavior and a better understanding of cyber criminal actions, the banking industry can take a proactive, holistic approach to potential threats.

$20.8 million average annualized cost of cybercrime in the financial services industry[8]

Is your cyber fraud and risk management solution able to stand up to the evolving threat landscape? Find out how you can stay ahead with this informative video.

To learn more about cyber fraud and risk management solutions for banks, visit Bottomline at www.bottomline.com or contact:

Phone: 800.472.1321
Email: info@bottomline.com

About Bottomline Technologies

Bottomline Technologies (NASDAQ: EPAY) powers mission-critical business transactions. We help our customers optimize financially-oriented operations and build deeper customer and partner relationships by providing a trusted and easy-to-use set of cloud-based digital banking, fraud prevention, payment, financial document, insurance, and healthcare solutions. Over 10,000 corporations, financial institutions, and banks benefit from Bottomline solutions. Headquartered in the United States, Bottomline also maintains offices in Europe and Asia-Pacific.

SOURCES:

[1] CNN, "Hackers Stole from 100 Banks and Rigged ATMs to Spew Cash," Feb. 16, 2015 http://money.cnn.com/2015/02/15/technology/security/kaspersky-bank-hacking/

[2] United States Department of the Treasury, FINCEN, "SAR Stats, Depository Institutions," April 2015 http://www.fincen.gov/news_room/rp/sar_by_number.html/

[3] Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and Abuse, 2014 Global Fraud Study* http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

[4] Ponemon Institute, *2014 Global Report on the Cost of Cyber Crime*, 2014 http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_mq32xtevyi

[5] Federal Financial Institutions Examinations Council, *Supplement to Authentication in an Internet Banking Environment*, 2011. http://www.ffiec.gov/pdf/Auth-ITS-Final%20 6-22-11%20(FFIEC%20Formated).pdf

[6] Information Security Media Group, *2013 Faces of Fraud: The Threat Evolution,* 2013 http://www.bankinfosecurity.com/handbooks.php?hb_id=49

[7] InformationWeek Bank Systems & Technology, "How Fraud & Cyber Security Will Evolve in 2015," Jan. 6, 2015 http://www.banktech.com/security/how-fraud-and-cyber-security-will-evolve-in-2015/a/d-id/1318489

[8] Ponemon Institute, *2014 Cost of Cyber Crime Study: United States*, October 2014, http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime

bottomline.com

Corporate Headquarters
Portsmouth, NH 03801 USA
tel 1.800.472.1321, +1.603.436.0700
email info@bottomline.com

Europe, Middle East, Africa
Reading, Berkshire RG17 JX UK
tel +44.118.925.8250
email emea-info@bottomline.com

Asia-Pacific
Hawthorn East, VIC, 3123 Australia
tel +61.3.9824.6888
email ap_info@bottomline.com