FIGHTING INTERNET TRANSACTION CRIMES: THE DIEBOLD WAY

Internet banking revenue lost more than **$3.5 BILLION** IN 2012 because of cyber criminals

EXECUTIVE SUMMARY

Technology has advanced greatly in the last few years in the financial services sector with Internet and mobile banking making it easy to access services on the go. But, as technology has become more sophisticated, so have criminals.

According to the CyberSource 2013 Fraud Report, online fraud in North America cost companies more than $3.5 billion in 2012, thanks to cyber criminals. That same report also indicated that the mobile channel posts the highest revenue fraud loss rate of 1.4 percent. A similar pattern exists globally.

With cyber crime rates on the rise around the world, financial institutions must adjust their strategies accordingly—but that does not seem to be happening fast enough in many cases. Occurrences are happening on a larger scale and more frequently, with end users often paying the biggest price.

CYBER SECURITY BECOMES MORE COMPLEX

Cyber criminals are masters of innovation. Every day they are finding new ways to gain unauthorized access to people's private information. With continuous improvement at the heart of every hacker, the number of endpoint cyber crime incidents, such as security breaches, malware installations on victim endpoints, successful phishing attacks and payment card fraud, is also increasing year after year.

That said, today's consumers are justifiably concerned about the security of their assets and information. In many cases, the end-user layer is the least protected. Anti-virus and spam blockers do not prevent sophisticated, targeted attacks on consumers.

Some particular attack types are gaining more traction of late. For example, exponential growth is being observed in the card not present (CNP) category, largely due to consumer adoption of online shopping. FICO reports that in the U.S. from 2011 to 2012, the CNP fraud incident rate grew by 25 percent and CNP fraud accounted for almost half (47 percent) of all credit card fraud. Further, the Websense 2013 Threat Report cited that deployment of malicious websites is regularly recording year-over-year growth in excess of 600 percent. To achieve this, hackers primarily redirect consumers to fake websites in attempts to gain access to private consumer information in a type of attack know as phishing.

Then, there's the explosion of smartphones, which is being propelled primarily by open technologies. The dark connotation of the word "open" here is that there are a lot of security gaps, proven by hackers in recent years. Research has shown that a significant number of mobile cyber attacks (involving malware installations, as the main attack type) are solely conducted to collect and profit from personal information of the users.

Cyber crime is indeed evolving. Just recently, a malware-hiding malware creator was discovered that was virtually undetectable by most anti-virus programs.

As attacks grow more prevalent, more sophisticated and larger in scale, consumers are forcing the hand of the financial institution to provide better endpoint protection, amid an already rapidly changing and challenging business environment.

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY

To save their reputations and long-term costs, financial institutions are realizing that they must stay a step ahead in terms of technology and real-time prevention to survive.

Traditionally, fraud-prevention measures were deployed by large financial institutions with the rest of the world following suit. A typical approach most organizations take to fighting cyber crime is upping their budgets for deploying cyber security measures. They buy the highest-cost technology or they purchase smaller solutions and try to make them work together. Not only are these expensive approaches, they often are unsuccessful.

Today's cyber criminals have become more nimble and are moving much faster than financial institutions. So, as the evolution continues, fighting cyber crime must be everyone's responsibility—regardless of size or geography. Cyber criminals often work together to carry out attacks. In turn, financial institutions employ that same type of solidarity to fight back. And processes must be flexible enough to enable immediate action against threats to servers—and end users.

Ultimately, the right solution must go beyond firewall systems, intrusion detection systems, anti-virus software, and Internet scanning programs.

Diebold's Online
ANTI-FRAUD SOLUTION
protects more than
40 MILLION
consumer endpoints 24/7

DIEBOLD'S ONLINE ANTI-FRAUD SOLUTION

Diebold, the trusted leader in financial security, understands how financial crimes are carried out and, more importantly, how to tackle them.

Diebold's Online Anti-Fraud Solution has been built to provide preventive protection to a consumer endpoint during the time of the transaction being conducted. By creating a virtual shielded environment for the user's endpoint (desktop, laptop or mobile), the solution provides enhanced protection against virtually all kinds of attacks. This solution has been proven to work in the real world, and today secures more than 40 million consumer endpoints around the clock.

By combining the power of an artificial intelligence technology with the solution, Diebold's Online Anti-Fraud Solution serves as a robust, end-to-end defense management system. The solution gets into action right at the beginning of a potential transaction and starts by authenticating the user endpoint as being a legitimate party accessing the financial institution's servers/website. These processes are customizable to the financial institution's policies. From that point on, the solution has just one important task to do: provide preventive protection until the consumer completes the transaction.

The Diebold solution has the ability to generate and process information about fraud and security violations among the co-participating financial institutions by means of a fraud information exchange, while preserving the privacy and confidentiality of financial institutions and end users.

Taking a comprehensive approach, Diebold's solution provides true integration among all of the channels used by the financial institution. Further, the solution has been engineered to be deployed as a plug-n-play add-on service, requiring zero to low customization to a financial institution's existing technological environment. This translates into the possibility of a quick and easy deployment, while having minimal disruptions to uptime.

CONCLUSION

According to the Ponemon Institute's 2013 Cost of Cyber Crime Study, organizations that deploy security intelligence technologies enjoyed an average cost savings of $4 million compared to those that did not.

By proactively offering a preventive protection solution to its consumers, financial institutions can build even greater trust and greater loyalty among its consumers, while actually saving money. You can't afford to not join the fight against cyber crime.

CONTACT INFORMATION:

Diebold, Inc.
P.O. Box 3077
Dept. 9-B-16
North Canton, Ohio 44720

For more information:
800.999.3600 USA
330.490.4000 International
www.diebold.com

DIEBOLD®