

WHITE PAPER

Smarter Security for Financial Networks with In-flight Optical Encryption

For the Financial Services Industry (FSI), cyber attacks have become one of the highest risks for regulatory violations and potential loss, exacerbated by the growing volume and sophistication of the attacks FSIs face. Failures in cybersecurity have the potential to impact a bank's operations, core systems, and reputation, and in the extreme can undermine the public's confidence in the individual bank as well as in the financial services industry as a whole. FSIs are increasingly dependent on Information and Communications Technology (ICT) to deliver services to their personal and business customers, which, as evidenced by recently publicized cyber hacking incidents, can place customer-specific information at risk of exposure.

The risk

The FSI finds itself under a seemingly never-ending barrage of cyber attacks on a daily basis. In fact, it holds the dubious honor of experiencing security incidents 300 percent more frequently than any other vertical¹, according to Forcepoint's 2015 Industry Drill-Down Report on Financial Services. More than 66 percent of financial institutions face at least one attack per year, and almost 15 percent face more than 100 per year, according to Help Net Security². With each attack carrying an average annualized cost of approximately \$16M USD³—the highest cost of any vertical, as reported by Ponemon's 2016 Cost of Cyber Crime study—it is little wonder security is a priority for most banking executives. According to Forbes,

this concern is evident in the fact that, in 2015, cybersecurity spending from four of the largest U.S. banks⁴—J.P. Morgan, Bank of America, Citigroup, and Wells Fargo—topped \$1.5B⁵, with the overall U.S. FSI laying out \$9.5B⁶.

This huge expense is hardly surprising when Ponemon reports⁷ that over half of their respondents had experienced malware, phishing attacks, Web-based attacks, malicious code, botnets, or stolen devices. This rise in the number and effectiveness of attacks is partly driven by the increasing ease and lower cost of staging an attack. There has been a proliferation in the use of increasingly less-costly hacking toolkits, with 64 percent of hackers rating them as 'Effective' or 'Highly Effective.'⁸

Ponemon's report found that more than 60 percent of hackers were deterred if the hack took more than 40 hours. However, as FSIs increase their defenses against these attacks but remain highly desirable targets, hackers will inevitably move to easier points of attack.

Why FSI CIOs do not encrypt in-flight data

Although FSIs have some of the largest deployments of encryption technology, typically these are deployed to protect data at rest, encrypting such caches as databases, data center storage arrays, and laptop hard drives. However, some CIOs do not fully realize the extent to which security has passed beyond their direct control once data leaves the premises.

¹ Forcepoint, *2015 Industry Drill-Down Report – Financial Services* www.forcepoint.com/content/2015-industry-drill-down-report

² <http://www.helpnetsecurity.com/2016/11/09/financial-institutions-cyber-attacks/>

³ Ponemon, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*

<http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf>

⁴ <http://www.bankrate.com/finance/banking/americas-biggest-banks-1.aspx>

⁵ <http://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boi-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#3cfab741112b>

⁶ Homeland Security Research Corp, "Banking & Financial Services Cybersecurity: U.S. Market 2015-2020 Report"

⁷ Ponemon, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* <http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf>

⁸ Ponemon/Palo Alto Networks, *Flipping the Economics of Attacks* – January 2016 <http://www.ponemon.org/blog/flipping-the-economics-of-attacks>